

Marques et copyright

Marques

Windows est une marque déposée de Microsoft Corporation aux États-Unis et dans d'autres pays.
Tous les autres noms de marques et de produits sont des marques ou marques déposées de leurs propriétaires respectifs.
Les marques protégées ne sont pas désignées comme telles dans le présent manuel. Cela ne signifie pas qu'elles peuvent être utilisées librement.

Remarques concernant le copyright

Des codes de fournisseurs tiers ont été utilisés pour Avira Antivirus Suite. Nous remercions les détenteurs des copyrights d'avoir mis leur code à notre disposition.
Vous trouverez de plus amples informations sur le copyright dans l'aide de Avira Antivirus Suite sous « Third Party Licenses ».

Contrat de licence d’utilisateur final (ci-après : « EULA »)

https://www.avira.com/fr/license-agreement

Politique de confidentialité

https://www.avira.com/fr/general-privacy



Sommaire









1. Introduction

Avec votre produit Avira, protégez votre ordinateur contre les virus, vers, chevaux de Troie, logiciels publicitaires et espions, et de tout autre risque. Ce manuel aborde de manière simplifiée les virus, logiciels malveillants et programmes indésirables.

Le manuel décrit l'installation et l'utilisation du programme.

Sur notre site Web, vous pouvez trouver différentes options et autres informations :

http://www.avira.com/fr

Sur le site Web d'Avira, vous pouvez :

- accéder aux informations concernant les autres produits d'Avira
- télécharger les derniers produits d'Avira
- télécharger les derniers manuels des produits au format PDF
- télécharger les outils de support et de réparation gratuits
- utiliser la vaste base de connaissances et les articles FAQ détaillés pour la résolution des problèmes
- accéder aux coordonnées du support en fonction des pays.

Votre équipe Avira

1.1 Symboles et mises en page

Les symboles suivants sont utilisés :

Symbole / Désignation	Explication
✓	Se trouve devant une condition à remplir avant d'exécuter une manipulation.
▸	Se trouve devant une manipulation que vous effectuez.



↳	Se trouve devant un résultat qui découle de la manipulation précédente.
Avertissement	Se trouve devant un avertissement en cas de risque de perte critique de données.
Remarque	Se trouve devant une remarque contenant des informations particulièrement importantes ou devant une astuce qui facilite la compréhension et l'utilisation de votre produit Avira.

Les mises en page suivantes sont utilisées :

Mise en page	Explication
Italique	Nom du fichier ou indication du chemin.
	Éléments de l'interface logicielle qui s'affichent (par ex. zone de fenêtre ou message d'erreur).
Gras	Éléments de l'interface logicielle sur lesquels vous cliquez (par ex. option de menu, rubrique, champ d'option ou bouton).

2. Informations produit

Ce chapitre vous donne toutes les informations importantes pour l'acquisition et l'utilisation de votre produit Avira :

- voir chapitre : Prestations
- voir chapitre : Configuration requise
- voir chapitre : Attribution de licence et mise à niveau
- voir chapitre : Gestion des licences

Les produits Avira proposent des outils complets et flexibles pour protéger votre ordinateur de manière fiable contre les virus, logiciels malveillants, programmes indésirables et autres dangers.

- Attention :

Avertissement
La perte de données précieuses a souvent des conséquences dramatiques. Même le meilleur programme de protection antivirus ne peut pas vous protéger à cent pour cent de la perte de données. Effectuez régulièrement des copies de sauvegarde (backup) de vos données.

Remarque
Un programme qui protège des virus, logiciels malveillants, programmes indésirables et autres dangers n'est fiable et efficace que s'il est à jour. Assurez-vous de l'actualité de votre produit Avira grâce aux mises à jour automatiques. Configurez le programme en conséquence.

2.1 Prestations

Votre produit Avira dispose des fonctions suivantes :

- Control Center pour la surveillance, la gestion et la commande de l'intégralité du programme
- Configuration centrale intuitive en mode standard ou expert avec une aide contextuelle
- Scanner (On-Demand Scan) avec recherche configurable par profil de tous les types connus de virus et logiciels malveillants
- Intégration au contrôle du compte d'utilisateur (User Account Control) de Windows pour pouvoir effectuer les tâches nécessitant des droits d'administrateur.
- Protection temps réel (On-Access Scan) pour la surveillance permanente de tous les accès aux données

- Composant ProActiv pour une surveillance permanente des actions de programme (uniquement pour systèmes 32 bits)
- Protection e-mail (scanner POP3, scanner IMAP et scanner SMTP) pour le contrôle permanent de vos e-mails à la recherche de virus et logiciels malveillants, notamment la vérification des pièces jointes
- Avira SearchFree Toolbar, une barre de recherche intégrée au navigateur Web vous permettant de faire des recherches rapides et faciles sur Internet. Elle contient également des widgets pour les principales fonctions d'Internet.
- Protection Web pour la surveillance des données et fichiers transmis par Internet par protocole HTTP (surveillance des ports 80, 8080, 3128)
- Avira Free Android Security est une application visant à empêcher la perte et/ou le vol de votre appareil. Elle vous aide à récupérer votre appareil mobile si vous l'avez perdu, ou pire, s'il vous a été volé. En outre, elle peut bloquer des appels entrants ou SMS. Avira Free Android Security protège les téléphones mobiles et smartphones dotés d'un système d'exploitation Android.
- Gestion de quarantaine intégrée pour l'isolation et le traitement des fichiers suspects
- Protection anti-rootkits pour la détection de logiciels malveillants dissimulés sur votre système (rootkits)
  (Non disponible sous Windows XP 64 bits)
- Accès direct aux informations détaillées sur les virus et logiciels malveillants trouvés via Internet
- Mise à jour simple et rapide du programme, des fichiers de définitions des virus (VDF) et du moteur de recherche grâce à la mise à jour de fichiers individuels et à la mise à jour incrémentielle VDF via un serveur Web basé sur Internet
- Gestion des licences simple et intuitive
- Planificateur intégré pour la définition de tâches uniques ou répétées comme les mises à jour et les contrôles
- Identification extrêmement efficace des virus et logiciels malveillants grâce à des technologies de recherche innovantes (moteur de scan) comprenant des procédés de recherche heuristique
- Identification de tous les types d'archives courants, y compris des extensions d'archives imbriquées et des extensions intelligentes
- Grande performance grâce à la capacité de multithreading (scannage simultané de nombreux fichiers à vitesse élevée)

2.2 Configuration requise

2.2.1 Configuration requise pour Avira Antivirus Suite

Avira Antivirus Suite requiert la configuration suivante pour pouvoir utiliser le système correctement :

Système d'exploitation

- Windows 8, dernier SP (32 ou 64 bits) ou
- Windows 7, dernier SP (32 ou 64 bits) ou
- Windows XP, dernier SP (32 ou 64 bits)

Matériel

- Processeur Pentium et supérieur, au moins 1 GHz
- 150 Mo minimum d'espace mémoire disponible sur le disque dur (voire plus pour la mémoire temporaire en cas d'utilisation de la fonction de quarantaine)
- 1024 Mo minimum de mémoire vive sous Windows 8, Windows 7
- 512 Mo minimum de mémoire vive sous Windows XP

Configuration supplémentaire

- Pour l'installation du programme : droits d'administrateur
- Pour toutes les installations : Windows Internet Explorer 6.0 ou une version ultérieure
- Connexion Internet le cas échéant (voir Préparation en vue de l'installation)

2.2.2 Configuration requise pour Avira SearchFree Toolbar

Conditions requises pour l'utilisation correcte de Avira SearchFree Toolbar :

Système d'exploitation

- Windows 8, dernier SP (32 ou 64 bits) ou
- Windows 7, dernier SP (32 ou 64 bits) ou
- Windows XP, dernier SP (32 ou 64 bits)

Navigateur Web

- Windows Internet Explorer 6.0 ou une version ultérieure
- Mozilla Firefox 3.0 ou une version ultérieure
- Google Chrome 18.0 ou une version ultérieure

> **Remarque**
> Si nécessaire, désinstallez les barres de recherche déjà installées avant d'installer Avira SearchFree Toolbar. Sinon, vous ne pourrez pas installer Avira SearchFree Toolbar.

2.2.3 Droits d'administrateur (à partir de Windows Vista)

Sous Windows XP, de nombreux utilisateurs travaillent avec des droits d'administrateur. Ceci n'est toutefois pas souhaitable pour des raisons de sécurité, car les virus et programmes indésirables peuvent plus facilement s'immiscer dans l'ordinateur.

C'est pourquoi Microsoft a mis en place le contrôle de compte d'utilisateur (UAC). Ce contrôle est intégré aux systèmes d'exploitation suivants :

- Windows Vista
- Windows 7
- Windows 8

Le contrôle de compte d'utilisateur offre une protection accrue aux personnes connectées en tant qu'administrateurs. Avec cette fonction, un administrateur ne dispose par défaut que des privilèges d'un utilisateur normal. Le système d'exploitation signale par une icône les actions pour lesquelles des droits d'administrateur sont nécessaires. En outre, l'utilisateur doit confirmer l'action souhaitée. Ce n'est qu'après avoir donné son accord que des privilèges plus importants sont octroyés et que le système d'exploitation exécute la tâche administrative en question.

Le produit Avira Antivirus Suite nécessite des droits d'administrateur pour certaines actions. Ces actions sont identifiées par le caractère suivant : . Si ce symbole apparaît sur un bouton, des droits d'administrateur sont nécessaires pour cette action. Si votre compte d'utilisateur actuel ne dispose pas de droits d'administrateur, la fenêtre de dialogue Windows du contrôle de compte d'utilisateur vous demande de saisir le mot de passe d'administrateur. Si vous ne disposez pas du mot de passe d'administrateur, vous ne pouvez pas exécuter cette action.

2.2.4 Incompatibilité avec d'autres programmes

Avira Antivirus Suite

Avira Antivirus Suite ne peut pour le moment pas être utilisé avec les produits suivants :

- PGP Desktop Home
- PGP Desktop Professional 9.0
- CyberPatrol

Un comportement erroné des produits mentionnés peut entraîner le non-fonctionnement de la Avira Protection e-mail (scanner POP3) d'Avira Antivirus Suite ou une instabilité du système. Avira cherche actuellement une solution au problème, en collaboration avec PGP et CyberPatrol. D'ici là, nous vous recommandons vivement de désinstaller les produits mentionnés avant d'installer Avira Antivirus Suite.

Avira Protection Web

Avira Protection Web n'est pas compatible avec les produits suivants :

- Teleport Pro de Tennyson Maxwell, Inc
- CHIPDRIVE® Time Recording de SCM Microsystems
- MSN Messenger de Microsoft

Les données envoyées et requises par ces produits sont donc ignorées par la Protection Web Avira.

> **Remarque**
> La Protection e-mail Avira ne peut pas fonctionner si un serveur email (par ex. AVM KEN, Exchange, ...) est déjà installé sur l'ordinateur.

2.3 Attribution de licence et mise à niveau

2.3.1 Attribution de licence

Pour pouvoir utiliser votre produit Avira, il vous faut une licence. Vous acceptez ainsi les conditions de licence.

La licence est attribuée sous forme d'un code d'activation. Le code d'activation est un code alphanumérique que vous recevez à l'achat du produit Avira. Les données exactes de votre licence sont enregistrées par le biais du code d'activation, c'est-à-dire pour quels programmes et pour combien de temps la licence vous a été accordée.

Le code d'activation vous est transmis par e-mail si vous avez acheté votre produit Avira sur Internet ou se trouve sur l'emballage du produit.

Pour obtenir la licence de votre programme, entrez le code d'activation lors de l'activation du programme. L'activation du produit peut s'effectuer lors de l'installation. Vous pouvez toutefois aussi activer votre produit Avira après l'installation dans le gestionnaire de licences sous **Aide > Gestion des licences**.

2.3.2 Prolongation de la licence

Si votre licence arrive prochainement à expiration, Avira vous rappelle de la prolonger par l'intermédiaire d'un message-bannière. Il vous suffit alors de cliquer sur un lien pour accéder à la boutique en ligne d'Avira. Vous pouvez également prolonger la licence de votre produit Avira dans le gestionnaire de licences, sous **Aide > Gestion des licences**.

Si vous êtes enregistré sur le portail de gestion des licences d'Avira, vous pouvez aussi prolonger votre licence dans l'**Aperçu des licences** ou opter pour la prolongation automatique.

2.3.3 Mise à niveau

Dans le gestionnaire de licences, vous avez la possibilité de lancer la mise à jour d'un produit issue de la gamme de produits Avira Desktop : vous n'avez donc pas besoin de procéder à une désinstallation manuelle de l'ancien produit et à une installation manuelle du nouveau produit. En cas de mise à niveau à partir du gestionnaire de licences, indiquez le code d'activation du produit auquel vous voulez passer dans le champ de saisie du gestionnaire de licences. Une installation automatique du nouveau produit s'effectue alors.

Afin de garantir une fiabilité et une protection élevées pour votre ordinateur, Avira vous rappelle la mise à jour en attente de la nouvelle version. Cliquez sur **Mise à jour** dans l'élément pop up pour accéder à la page de mise à jour spécifique au produit. Vous pouvez effectuer une mise à jour de votre produit actuel ou acquérir un produit Avira avec davantage de fonctionnalités. La page d'aperçu des produits Avira vous montre le produit que vous utilisez actuellement et vous donne la possibilité de le comparer à d'autres produits Avira. Pour davantage d'informations, cliquez sur l'icône d'information à droite à côté du nom du produit. Si vous souhaitez conserver votre produit actuel, cliquez sur **Mise à jour** pour installer immédiatement la version la plus récente avec des fonctions optimisées. Pour acheter un produit plus complet, cliquez sur **Acheter** en bas de la colonne du produit concerné. Vous êtes dirigé vers la boutique en ligne Avira pour procéder à votre commande.

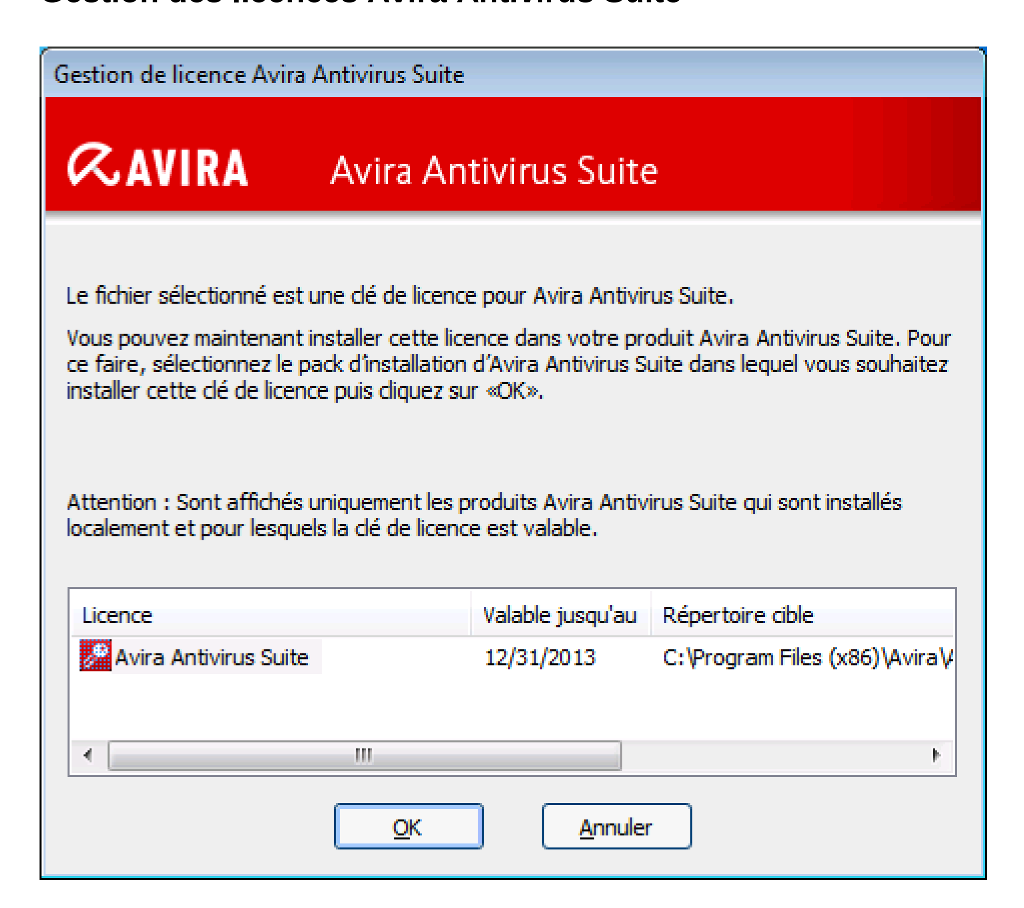
Remarque
Selon votre produit et votre système d'exploitation, vous devez éventuellement disposer des droits d'administrateur pour procéder à cette mise à jour. Connectez-vous en tant qu'administrateur avant d'effectuer une mise à jour.

2.3.4 Gestion des licences

La gestion des licences Avira Antivirus Suite permet une installation très simple de la licence Avira Antivirus Suite.



Gestion des licences Avira Antivirus Suite



Vous pouvez effectuer une installation de la licence en sélectionnant le fichier de licence dans votre gestionnaire de fichiers ou l'e-mail d'activation en cliquant deux fois dessus et en suivant les instructions à l'écran.

Remarque
La gestion des licences Avira Antivirus Suite copie la licence correspondante automatiquement dans le dossier de produit correspondant. Si une licence est déjà disponible, un message s'affiche demandant si le fichier de licence doit être remplacé. Dans ce cas, le fichier déjà existant est écrasé avec le fichier de licence actuel.

3. Installation et désinstallation

3.1 Installation et désinstallation

Ce chapitre vous propose des informations sur l'installation de Avira Antivirus Suite.

- Préparation en vue de l'installation
- Installation à partir du CD en ligne
- Installation à partir du CD hors ligne
- Installation des logiciels téléchargés
- Suppression des logiciels incompatibles
- Sélection du type d'installation
- Installation de Avira Antivirus Suite
- Modification de l'installation
- Désinstallation de Avira Antivirus Suite

3.2 Préparation en vue de l'installation

✓ Avant de procéder à l'installation, vérifiez si votre ordinateur affiche la configuration requise.
✓ Fermez toutes les applications en cours.
✓ Assurez-vous qu'aucune autre solution antivirus n'est installée. Les fonctions de protection automatiques des différentes solutions de sécurité peuvent entrer en conflit (voir Suppression de logiciels incompatibles au sujet des options automatiques).
✓ Si nécessaire, désinstallez les barres de recherche déjà installées avant d'installer Avira SearchFree Toolbar. Sinon, vous ne pourrez pas installer Avira SearchFree Toolbar.
✓ Connectez-vous à Internet.

- La connexion est nécessaire à l'exécution des étapes d'installation suivantes :
  - Téléchargement des fichiers de programme actuels et du moteur de recherche, ainsi que des fichiers de définitions des virus à jour par le biais du programme d'installation (en cas d'installation à partir d'Internet)
  - Activation du programme
  - Enregistrement en tant qu'utilisateur
  - Si nécessaire, exécution d'une mise à jour une fois l'installation terminée

✓ Ayez le code d'activation ou le fichier de licence du produit Avira Antivirus Suite à disposition lorsque vous souhaitez activer le programme
✓ Avira Antivirus Suite utilise le protocole HTTP et le port 80 (de communication Web) ainsi que le protocole de chiffrement SSL et le port 443, pour communiquer avec les serveurs Avira en vue de l'activation ou de l'enregistrement du produit. Si vous



utilisez un pare-feu, assurez-vous que celui-ci ne bloque pas les connexions nécessaires ni les données entrantes ou sortantes.

3.3 Installation à partir du CD en ligne

- Insérez le CD Avira Antivirus Suite.

Cliquez sur **Ouvrir un dossier** pour visualiser les fichiers si le démarrage automatique est activé.
OU

Accédez à votre lecteur CD, cliquez sur AVIRA avec le bouton droit de la souris puis sélectionnez **Ouvrir un dossier** pour visualiser les fichiers.

Double-cliquez sur le fichier *autorun.exe*.

Dans le menu CD, sélectionnez la version en ligne à installer.

Le programme recherche les logiciels incompatibles (plus d'infos ici : Suppression des logiciels incompatibles).

Cliquez sur **Suivant** dans l'écran *Bienvenue*.

Sélectionnez la langue puis cliquez sur **Suivant**. Tous les fichiers nécessaires à l'installation sont téléchargés à partir des serveurs Web Avira.

Poursuivez avec Sélection du type d'installation.

3.4 Installation à partir du CD hors ligne

- Insérez le CD Avira Antivirus Suite.

Cliquez sur **Ouvrir un dossier** pour visualiser les fichiers si le démarrage automatique est activé.
OU

Accédez à votre lecteur CD, cliquez sur AVIRA avec le bouton droit de la souris puis sélectionnez **Ouvrir un dossier** pour visualiser les fichiers.

Double-cliquez sur le fichier *autorun.exe*.

Dans le menu du CD, sélectionnez la version hors ligne à installer.

Le programme recherche les logiciels incompatibles (plus d'infos ici : Suppression des logiciels incompatibles).

Le fichier d'installation est décompressé. La routine d'installation démarre.

Poursuivez avec Sélection du type d'installation.

3.5 Installation des logiciels téléchargés depuis la boutique Avira

- Accédez à la page www.avira.com/download.

Sélectionnez le produit puis cliquez sur **Télécharger**.

Enregistrez le fichier téléchargé sur votre ordinateur.

Double-cliquez sur le fichier d'installation Avira Antivirus Suite_(fr).exe.

Si la fenêtre de dialogue Windows du contrôle de compte d'utilisateur apparaît, cliquez sur Oui.

Le programme recherche les logiciels incompatibles (plus d'infos ici : Suppression des logiciels incompatibles).

Le fichier d'installation est décompressé. La routine d'installation démarre.

Poursuivez avec Sélection du type d'installation.

3.6 Suppression des logiciels incompatibles

Avira Antivirus Suite parcourt votre système pour détecter d'éventuels programmes incompatibles. Quand Avira Antivirus Suite identifie des logiciels incompatibles, il génère la liste de ces programmes. Nous vous recommandons de désinstaller ces programmes afin de ne pas compromettre la sécurité de votre ordinateur.

- Dans cette liste, sélectionnez les programmes devant être supprimés automatiquement de votre ordinateur et cliquez sur **Suivant**.

La désinstallation de certains produits doit être confirmée manuellement.

Sélectionnez les programmes puis cliquez sur **Suivant**.

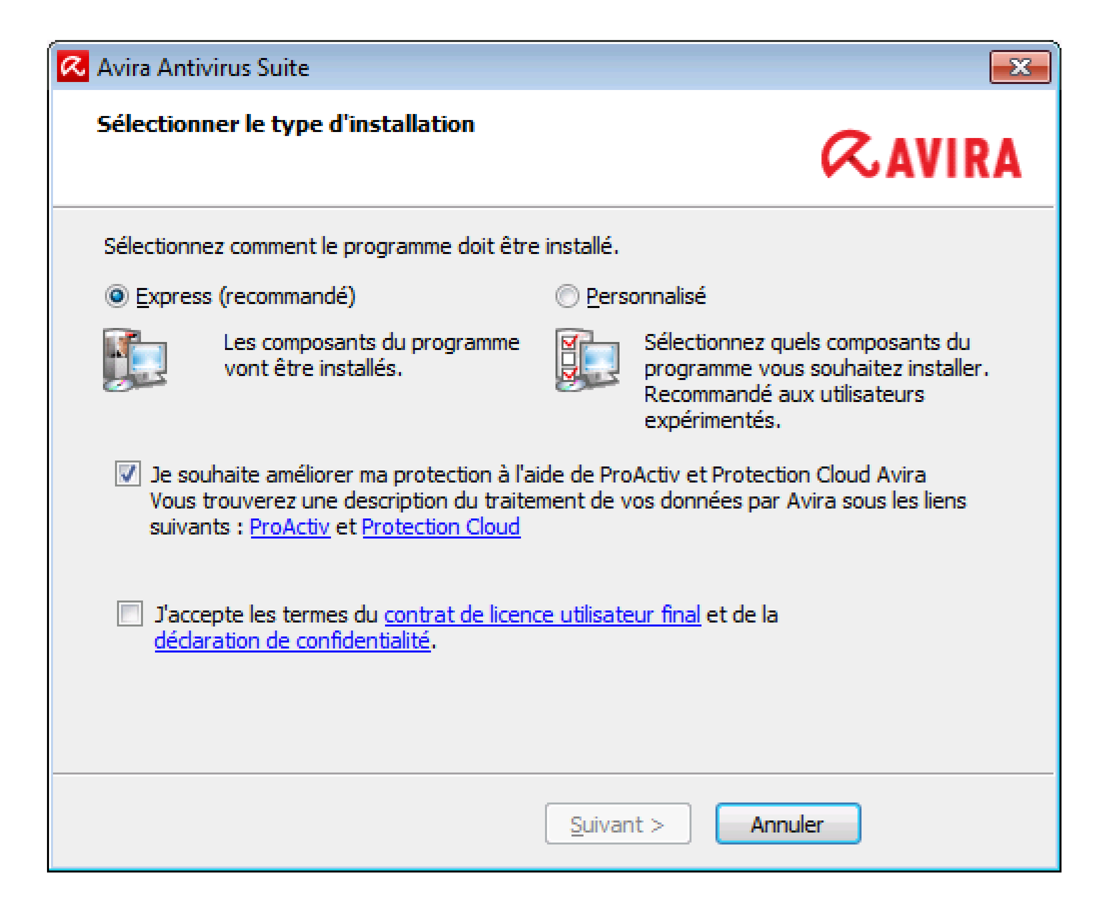
La désinstallation d'un ou plusieurs programmes sélectionnés peut nécessiter le redémarrage de l'ordinateur. L'installation est lancée après le redémarrage.

3.7 Sélection du type d'installation

3.7.1 Sélection du type d'installation

Pendant l'installation, vous pouvez choisir un type de configuration dans l'assistant d'installation. L'assistant d'installation est conçu pour vous guider tout au long de l'installation.





Thèmes apparentés :

- voir Exécution d'une installation expresse
- voir Exécution d'une installation personnalisée

3.7.2 Exécution d'une installation expresse

L'*installation expresse* correspond à la routine d'installation recommandée.

- Elle installe les composants standard de Avira Antivirus Suite. Les paramètres de niveau de sécurité Avira recommandés sont utilisés.
- Un des chemins d'installation suivants est sélectionné par défaut :
  - *C:\Program Files\Avira* (pour les versions Windows 32 bits) ou
  - *C:\Program Files (x86)\Avira* (pour les versions Windows 64 bits)
- Vous y trouverez tous les fichiers associés à Avira Antivirus Suite.
- Si vous choisissez ce type d'installation, il vous suffit de cliquer sur **Suivant** jusqu'à son terme pour exécuter une installation.
- Ce type d'installation est spécialement conçu pour les utilisateurs qui ne se sentent pas aptes à configurer des outils logiciels.



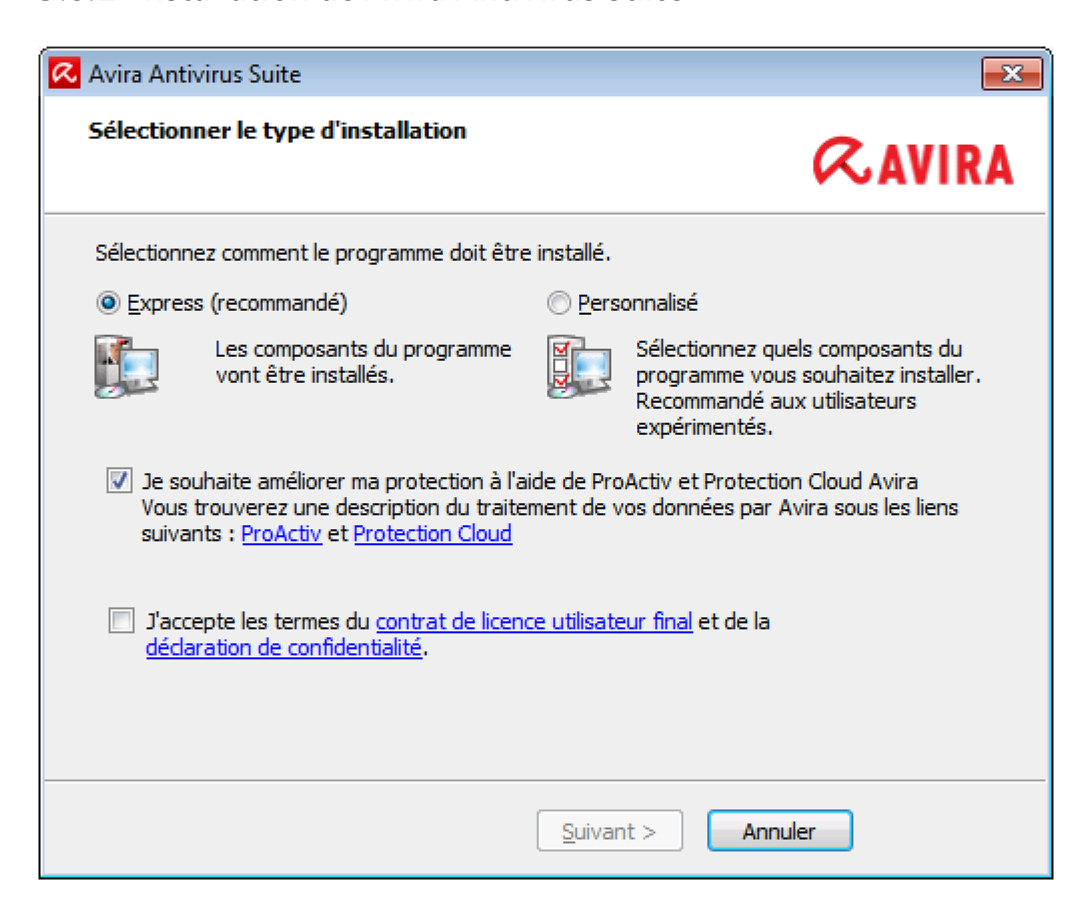
3.7.3 Exécution d'une installation personnalisée

L'*Installation personnalisée* vous permet de configurer votre installation. Ceci est recommandé uniquement pour les utilisateurs avancés qui disposent de connaissances approfondies en matière de matériel informatique et de logiciels ainsi que de sécurité.

- Vous pouvez choisir d'installer les divers composants du programme.
- Vous pouvez sélectionner un répertoire de destination pour les fichiers de programme à installer.
- Vous pouvez désactiver l'option de **création d'un raccourci sur le Bureau et/ou d'un groupe de programmes dans le menu Démarrer**.
- Vous pouvez utiliser l'assistant de configuration pour définir des paramètres personnalisés pour le produit Avira Antivirus Suite. Vous pouvez également sélectionner le niveau de sécurité qui vous convient.
- Une fois l'installation terminée, vous pouvez lancer un contrôle rapide du système qui est exécuté automatiquement à l'issue de l'installation.

3.8 Installation d'Avira Antivirus Suite

3.8.1 Installation de Avira Antivirus Suite



- Si vous ne souhaitez pas participer à la communauté Avira, désélectionnez la case **Je souhaite améliorer ma protection avec Avira ProActiv et Protection Cloud**, qui est activée par défaut.

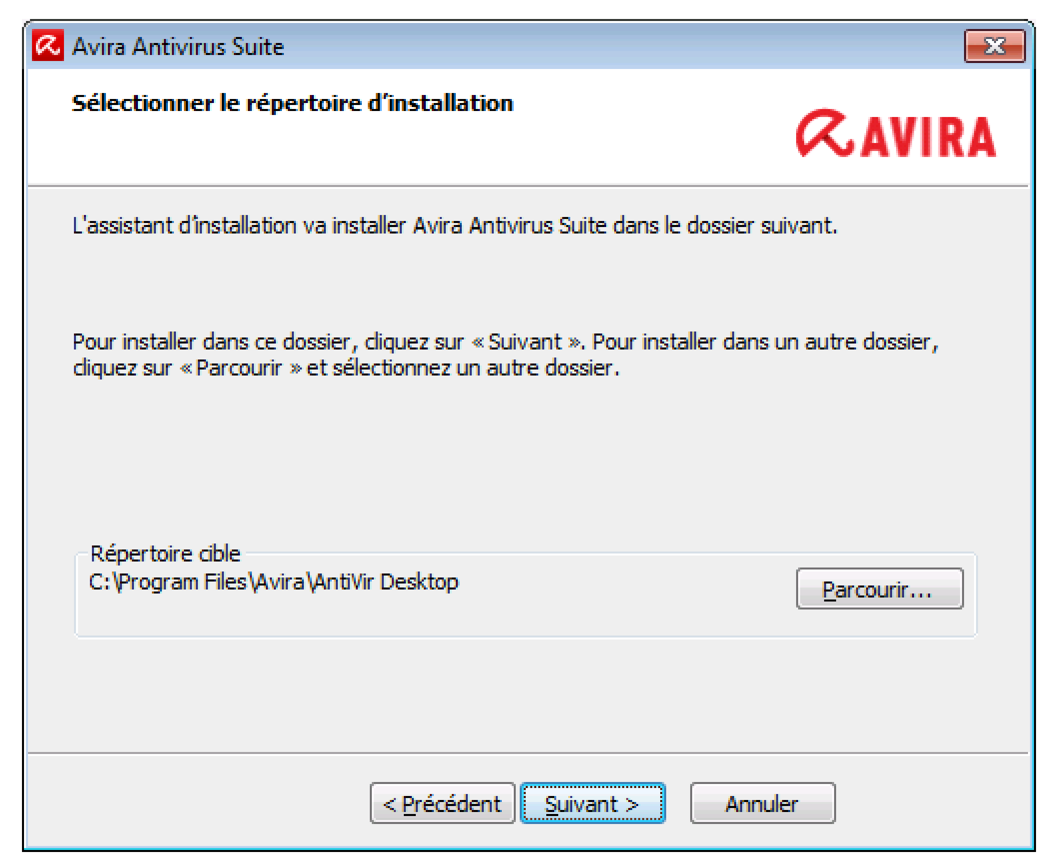
  Si vous confirmez votre participation à la communauté Avira, Avira Antivirus Suite envoie les données sur les programmes suspects détectés au Avira Centre de recherche sur les logiciels malveillants. Les données servent uniquement à une analyse en ligne avancée et au développement et à l'amélioration de la technologie de détection.

  Vous pouvez cliquer sur les liens **ProActiv** et **Protection Cloud** pour obtenir de plus amples détails sur l'analyse en ligne et dans le cloud améliorée.

  Confirmez que vous acceptez le **contrat de licence utilisateur final**. Pour lire l'intégralité du **contrat de licence utilisateur final**, cliquez sur le lien correspondant.

3.8.2 Sélection du dossier de destination

L'installation personnalisée vous permet de sélectionner le dossier où vous souhaitez installer Avira Antivirus Suite.



- Cliquez sur **Parcourir** puis accédez à l'emplacement où vous souhaitez installer Avira Antivirus Suite.

  Sélectionnez le dossier dans lequel vous souhaitez installer Avira Antivirus Suite dans la fenêtre **Sélectionner le dossier de destination**.



Cliquez sur **Suivant**.

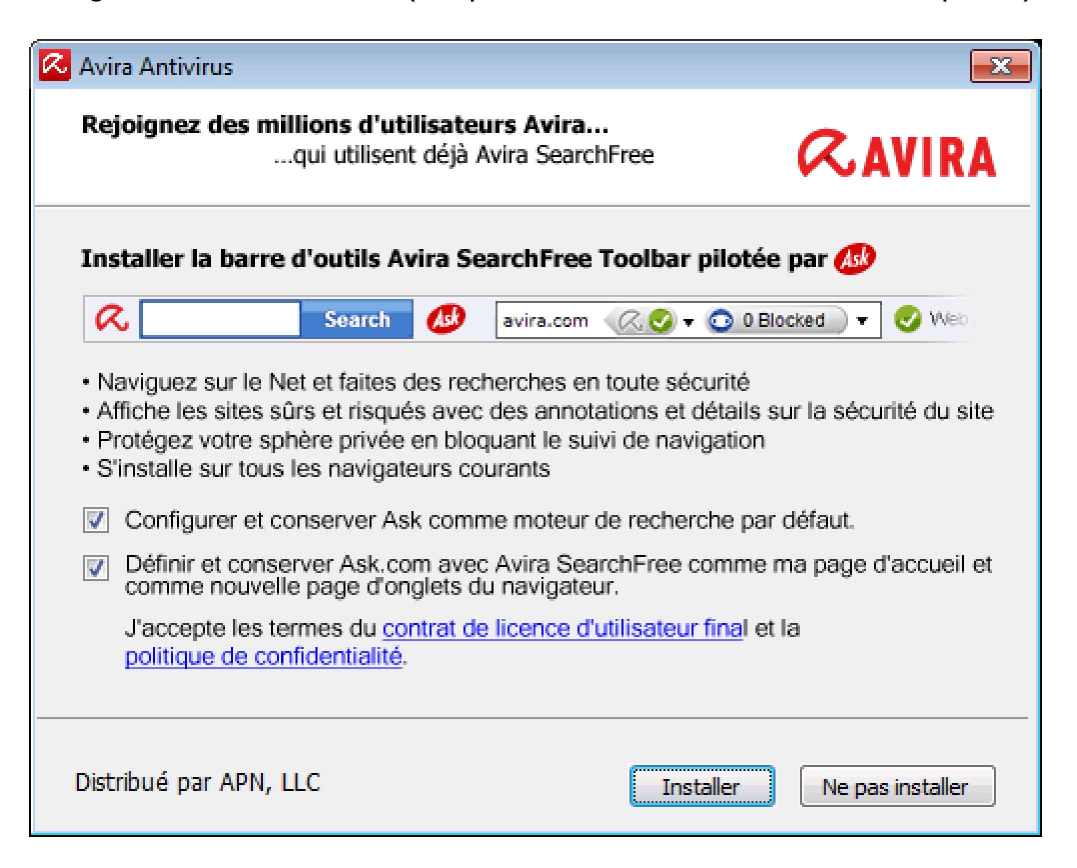
3.8.3 Installation de Avira SearchFree Toolbar

Vous pouvez installer Avira SearchFree Toolbar à l'issue de l'installation.

Avira SearchFree Toolbar comprend deux principaux composants : Avira SearchFree et Toolbar.

Avira SearchFree vous permet de rechercher un certain nombre d'éléments sur Internet. Le moteur de recherche affiche tous les résultats dans la fenêtre de navigateur en évaluant leur niveau de sécurité. Il permet aux utilisateurs Avira de naviguer dans de meilleures conditions de sécurité sur Internet.

Toolbar vous offre trois widgets pour accéder directement aux fonctions importantes sur Internet. En un clic, accédez directement à Facebook, votre messagerie ou à une navigation Web sécurisée (uniquement sur Firefox et Internet Explorer).

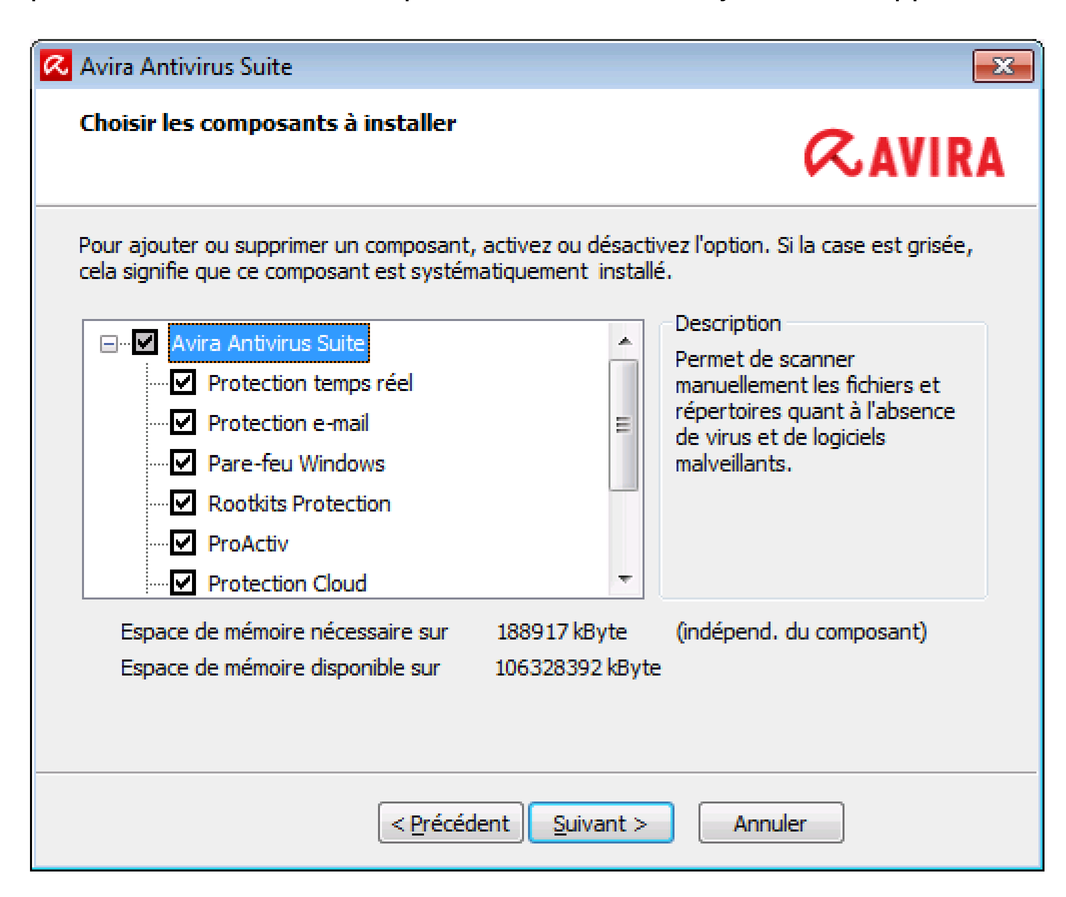


Si vous ne souhaitez pas installer Avira SearchFree Toolbar, désactivez les cases des options **Définir et conserver Ask comme mon fournisseur de recherche par défaut** et **Définir et conserver Avira SearchFree (avira.search.ask.com) comme ma page d'accueil de navigateur et la page de nouveaux onglets de navigateur**.

Si vous refusez, seul le programme d'installation Avira SearchFree Toolbar sera annulé. L'installation de Avira Antivirus Suite sera toutefois menée à son terme.

3.8.4 Sélection des composants d'installation

Lors d'une installation personnalisée ou modifiée, les composants d'installation suivants peuvent être sélectionnés pour l'installation, ou ajoutés ou supprimés.



Sélectionnez ou désélectionnez les composants dans la liste présentée dans la fenêtre de dialogue Installer les composants.

- **Avira Antivirus Suite**
  Ceci contient tous les composants nécessaires à l'installation correcte du produit Avira Antivirus Suite.
  - **Protection temps réel**
    Avira Protection temps réel fonctionne en arrière-plan. Il surveille et répare si possible les fichiers lors d'opérations comme l'ouverture, l'écriture et la copie en temps réel (On-Access = à l'accès). Le mode en temps réel signifie que si un utilisateur effectue une opération sur le fichier (charger, exécuter ou copier le fichier), Avira Antivirus Suite parcourt automatiquement le fichier. Renommer un fichier ne déclenche toutefois pas l'analyse réalisée par Avira Protection temps réel.
  - **Protection e-mail**
    Protection e-mail sert d'interface entre votre ordinateur et le serveur e-mail à partir duquel votre programme de messagerie (client de messagerie) télécharge les e-mails. Protection e-mail sert de proxy entre le programme de messagerie et le serveur e-mail. Tous les e-mails entrants sont transférés via ce proxy, la présence de virus et de programmes indésirables est recherchée, puis ils sont transmis à votre



programme de messagerie. Selon la configuration, le programme traite les e-mails automatiquement ou vous demande de préciser l'opération à exécuter.

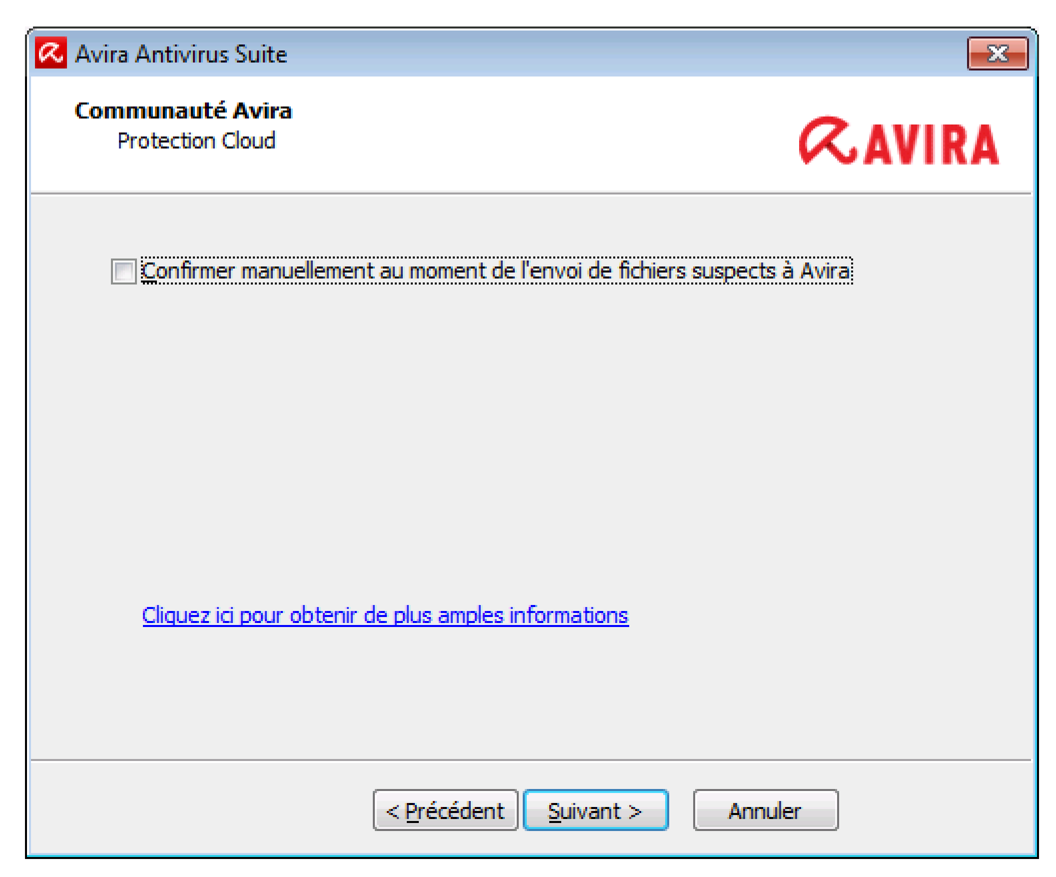
- **Pare-feu Windows** (à partir de Windows 7)
  Ce composant gère le pare-feu Windows depuis Avira Antivirus Suite.
- **Protection Rootkits**
  Avira Protection Rootkits vérifie la présence de logiciels sur votre ordinateur qui ne peuvent plus être détectés par les méthodes conventionnelles de protection anti-logiciel malveillant après s'être introduits dans le système informatique.
- **ProActiv**
  Le composant ProActiv surveille les actions des applications et alerte les utilisateurs en cas de comportement suspect. Grâce à cette détection basée sur le comportement, vous pouvez vous protéger contre des logiciels malveillants inconnus. Le composant ProActiv est intégré dans Avira Protection temps réel.
- **Protection Cloud**
  Le composant Protection Cloud est un module de détection dynamique en ligne de logiciels malveillants encore inconnus. Ceci signifie que les fichiers sont chargés à un emplacement distant et comparés à des fichiers connus ainsi qu'à d'autres fichiers en cours de chargement et d'analyse en temps réel (non programmés et sans délai). Ceci permet de maintenir la base de données constamment à jour afin de fournir un meilleur niveau de sécurité.
  Si vous avez choisi d'installer le composant Protection Cloud, mais que vous souhaitez confirmer manuellement à chaque fois les fichiers devant être envoyés vers le Cloud pour analyse, vous pouvez activer l'option **Confirmer manuellement l'envoi des fichiers suspects à Avira.**
- **Protection Web**
  En navigant sur Internet, via votre navigateur Internet, vous sollicitez des données d'un serveur Web. Les données transmises par le serveur Web (fichiers HTML, script et images, fichiers flash, flux vidéo et musique, etc.) arrivent normalement directement dans la mémoire cache du navigateur, pour être exécutées dans le navigateur Internet, ce qui exclut un contrôle par une recherche en temps réel comme Avira Protection temps réel le propose. De cette manière, des virus et programmes indésirables peuvent pénétrer dans votre système. Protection Web est un proxy HTTP qui surveille les ports (80, 8080, 3128) servant à la transmission des données et contrôle l'absence de virus et de programmes indésirables dans les données transférées. Selon la configuration, le programme traite les fichiers concernés automatiquement ou demande à l'utilisateur quelle action entreprendre.
- **Extension d'environnement**
  L'extension d'environnement génère une entrée **Contrôler les fichiers sélectionnés avec Avira** dans le menu contextuel de Windows Explorer (cliquer avec le bouton droit de la souris). Cette entrée vous permet de contrôler directement des fichiers ou des répertoires.

Thèmes apparentés :
Modification de l'installation



3.8.5 Envoi de fichiers suspects à Avira Protection Cloud

Si vous souhaitez participer à la communauté Avira, vous pouvez choisir de confirmer manuellement le téléchargement à chaque fois qu'un fichier doit être envoyé à Avira Centre de recherche sur les logiciels malveillants.

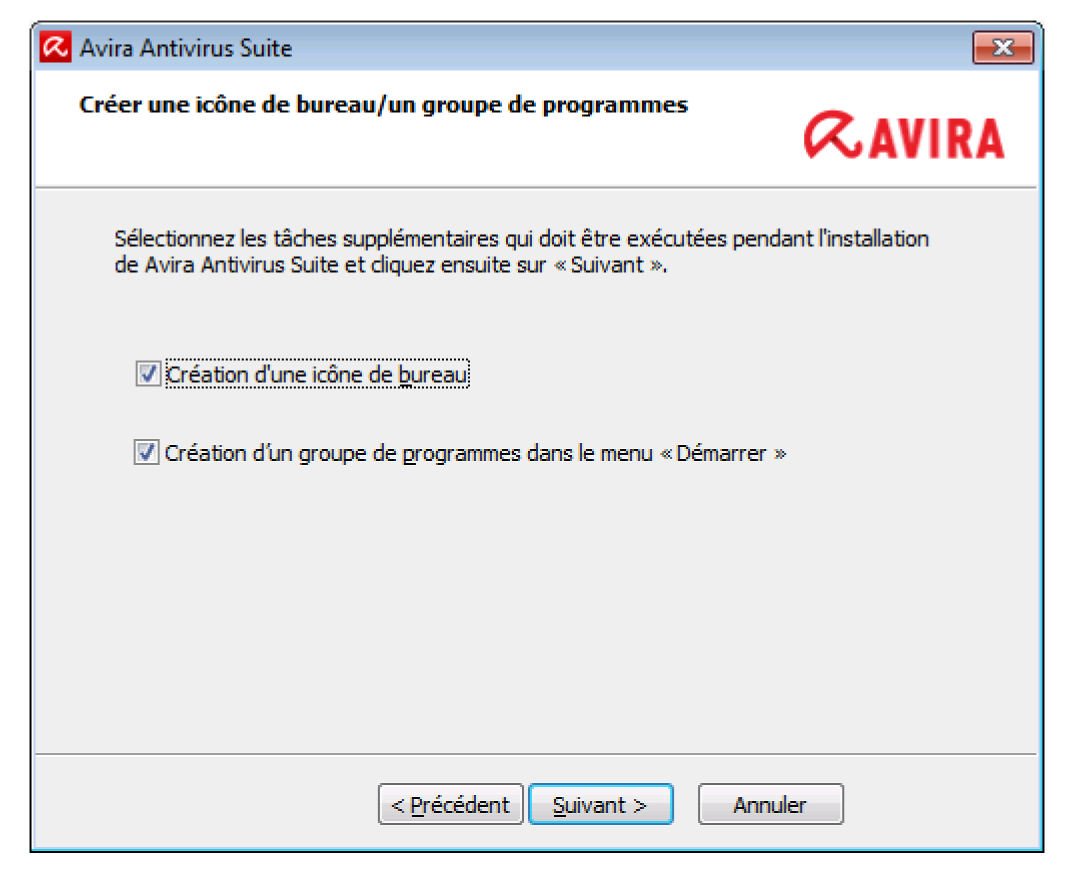


- Afin que Avira Antivirus Suite demande la confirmation à chaque fois, activez l'option **Confirmer manuellement lors de l'envoi de fichiers suspects à Avira**.

3.8.6 Création de raccourcis pour Avira Antivirus Suite

Une icône de bureau et/ou un groupe de programme dans le menu Démarrer vous aideront à accéder à Avira Antivirus Suite plus rapidement et facilement.



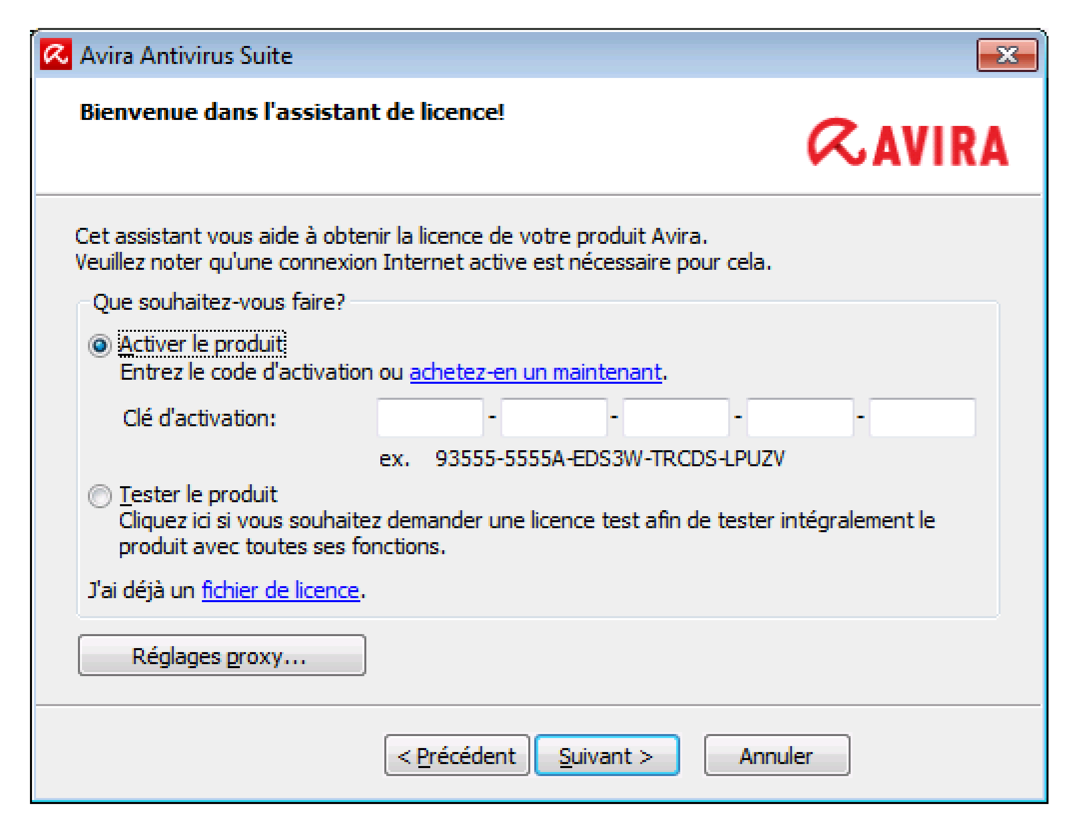


- Pour créer un raccourci de bureau pour Avira Antivirus Suite et/ou un groupe de programmes dans le **Menu Démarrer**, laissez la ou les options correspondantes activées.

3.8.7 Activation de Avira Antivirus Suite

Plusieurs méthodes s'offrent à vous pour activer Avira Antivirus Suite.





Si vous avez déjà reçu un code d'activation, saisissez le code d'activation dans les champs proposés.

- Si vous ne disposez pas encore d'un code d'activation, cliquez sur le lien pour en acheter un.

  Vous êtes dirigé vers le site Web Avira où vous pouvez acheter un code d'activation.

- Si vous souhaitez seulement évaluer le produit, sélectionnez **Tester le produit** et insérez vos données dans les champs requis à des fins d'enregistrement.

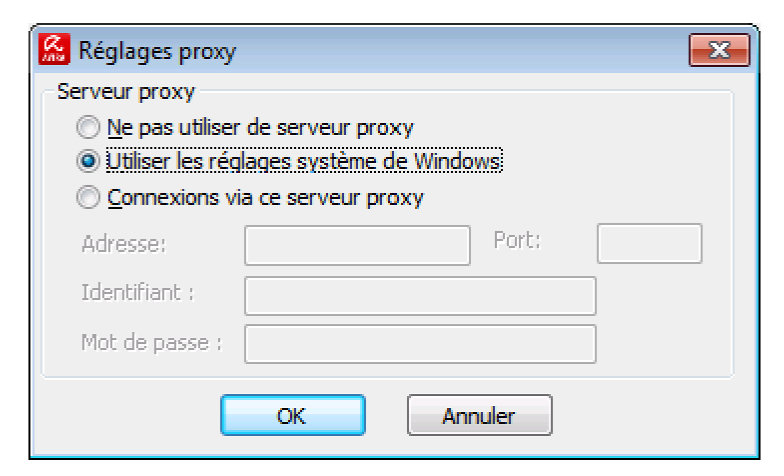
  Votre licence d'évaluation est valable pendant 31 jours.

- Si vous avez déjà activé un produit et souhaitez réinstaller votre produit Avira, sélectionnez l'option **Je possède déjà un fichier de licence valide**.

  Une fenêtre de navigateur s'ouvre et vous pouvez naviguer vers le fichier *hbedv.key* sur votre ordinateur.

3.8.8 Définition des paramètres proxy

La définition des paramètres proxy est recommandée uniquement pour les utilisateurs avancés qui disposent de connaissances approfondies en matière de matériel informatique, de logiciels et de sécurité.



- S'il n'est pas prévu de connecter Avira Antivirus Suite à Internet via un serveur proxy, activez l'option **Ne pas utiliser de serveur proxy**.
- Si vous voulez que Avira Antivirus Suite se connecte à Internet comme toute autre application installée, laissez l'option **Utiliser les paramètres système Windows** activée (l'option est activée par défaut).

  Vous pouvez configurer les paramètres système de Windows pour l'utilisation d'un serveur proxy sous **Panneau de configuration > Options Internet > Connexions > Paramètres LAN**. Vous pouvez également accéder aux options Internet dans le menu **Outils** d'Internet Explorer.

> **Remarque**
> Si vous utilisez un serveur proxy qui exige une authentification, renseignez les données complètes requises sous l'option **Connexion via ce proxy**. L'option **Utiliser les paramètres système de Windows** ne peut être utilisée que pour les serveurs proxy sans authentification.

- Pour configurer un serveur proxy spécialement associé à Avira Antivirus Suite, activez l'option **Connexion via ce proxy** puis renseignez les informations demandées :

Adresse

Saisissez le nom de l'ordinateur ou l'adresse IP du serveur proxy que vous souhaitez utiliser pour la connexion au serveur Web.

Exemples :

Adresse : proxy.domain.com

Adresse : 192.168.1.100

Port

Veuillez saisir le numéro de port du serveur proxy que vous souhaitez utiliser pour la connexion au serveur Web.

Exemples :



Port : 8080

Port : 3128

Identifiant de connexion

Saisissez un identifiant pour la connexion au serveur proxy.

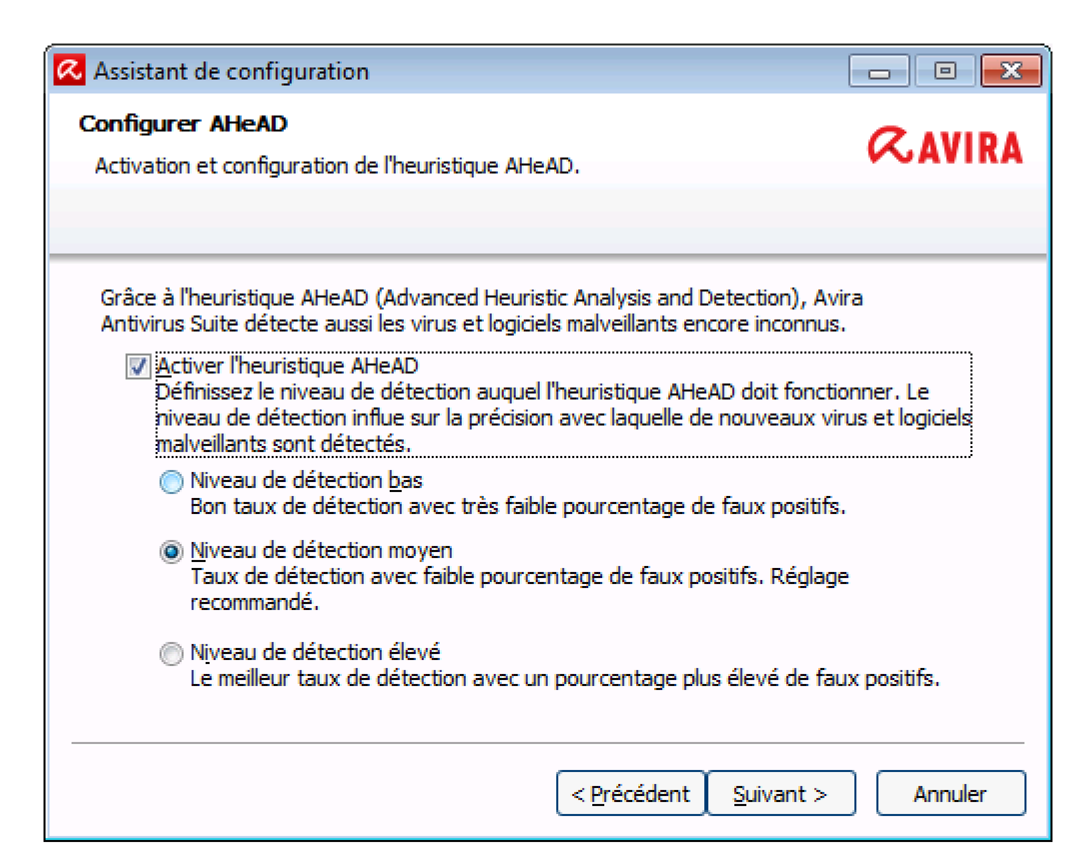
Mot de passe de connexion

Saisissez le mot de passe correspondant pour la connexion au serveur proxy. Le mot de passe est mémorisé de manière chiffrée. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Cliquez sur **OK**.

3.8.9 Configuration du niveau de détection heuristique (AHeAD)

Avira Antivirus Suite contient un outil très performant faisant appel à la technologie Avira AHeAD (*Advanced Heuristic Analysis and Detection*). Cette technologie met en œuvre des techniques de reconnaissance de formes qui lui permettent de détecter les (nouveaux) logiciels malveillants inconnus à partir des analyses précédentes d'autres logiciels malveillants.



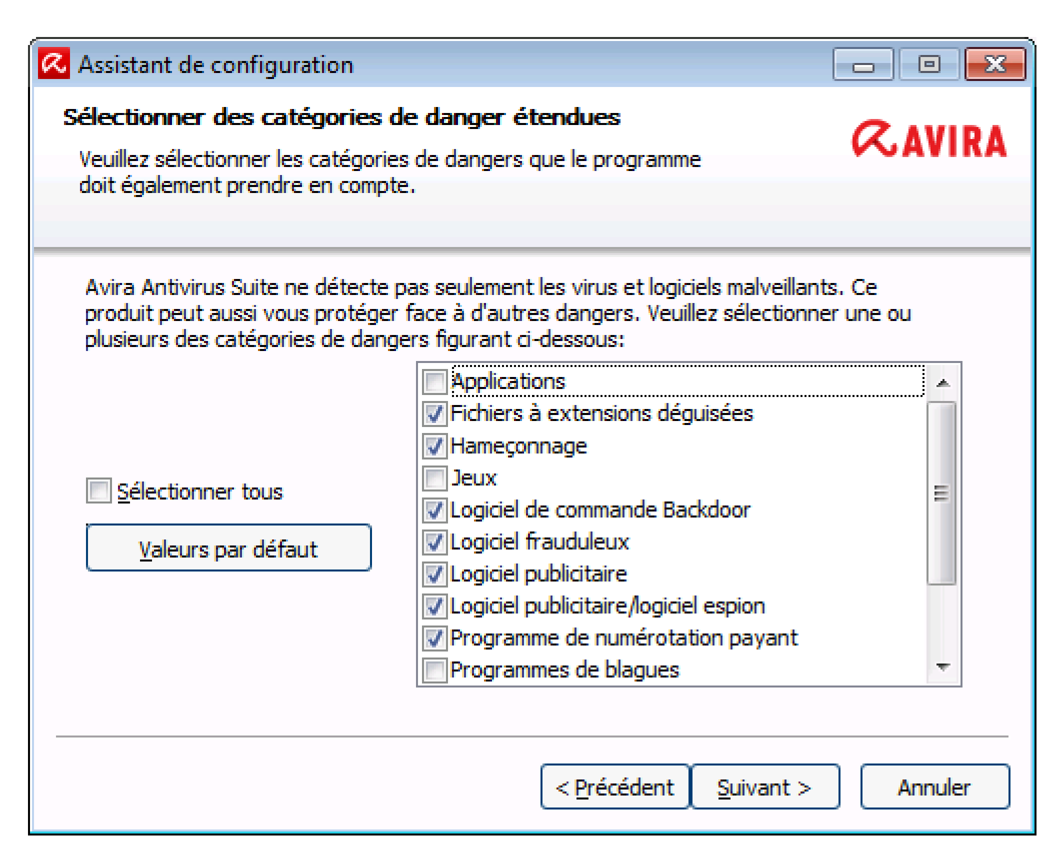
- Sélectionnez un niveau de détection dans la fenêtre de dialogue **Configurer AHeAD** puis cliquez sur **Suivant**.



Le niveau de détection choisi est utilisé pour le paramétrage de la technologie AHeAD Scanner (recherche directe) et Protection temps r�el (recherche en temps réel).

3.8.10 Sélection de catégories de danger étendues

Les virus et les logiciels malveillants ne sont pas les seuls éléments représentant un danger pour votre système informatique. Nous avons défini une liste complète de risques et les avons classés en catégories de menace étendues à votre attention.



- Un certain nombre de catégories de menace est déjà sélectionné par défaut.

  Le cas échéant, sélectionnez des catégories de danger supplémentaires dans la fenêtre de dialogue **Sélectionner des catégories de danger étendues**.

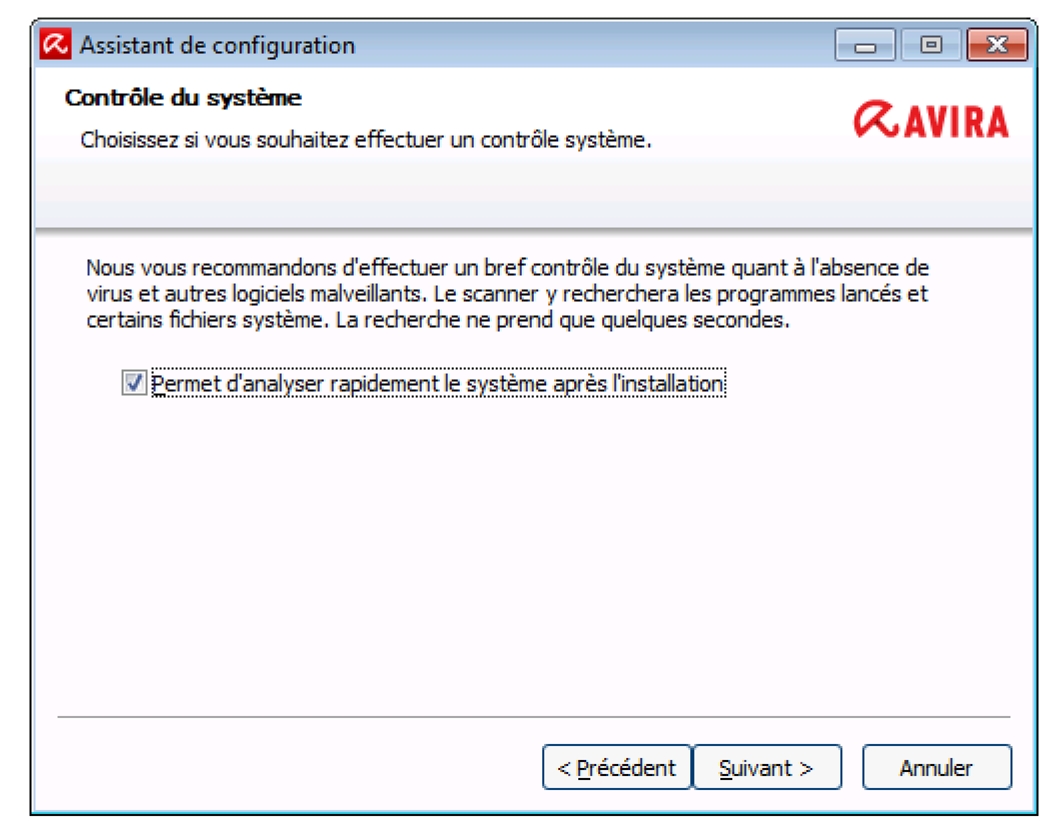
  Si vous changez d'avis, vous pouvez rétablir les valeurs recommandées en cliquant sur le bouton **Valeurs par défaut**.

  Poursuivez l'installation en cliquant sur **Suivant**.

3.8.11 Démarrage d'une analyse après l'installation

Pour vérifier l'état de sécurité actuel de l'ordinateur, un contrôle rapide du système peut être exécuté à l'issue de la configuration et avant le redémarrage de l'ordinateur. Le Scanner parcourt les programmes lancés et les fichiers système les plus importants, à la recherche de virus et de logiciels malveillants.





- Si vous souhaitez exécuter un contrôle rapide du système, laissez l'option **Quick System Scan** activée.

  Cliquez sur **Suivant**.

  Terminez la configuration en cliquant sur **Terminer**.

  Si vous n'avez pas désactivé l'option **Quick System Scan**, la fenêtre *Luke Filewalker* s'ouvre.

  Le Scanner effectue un contrôle rapide du système.

3.9 Modification de l'installation

3.9.1 Modification de l'installation

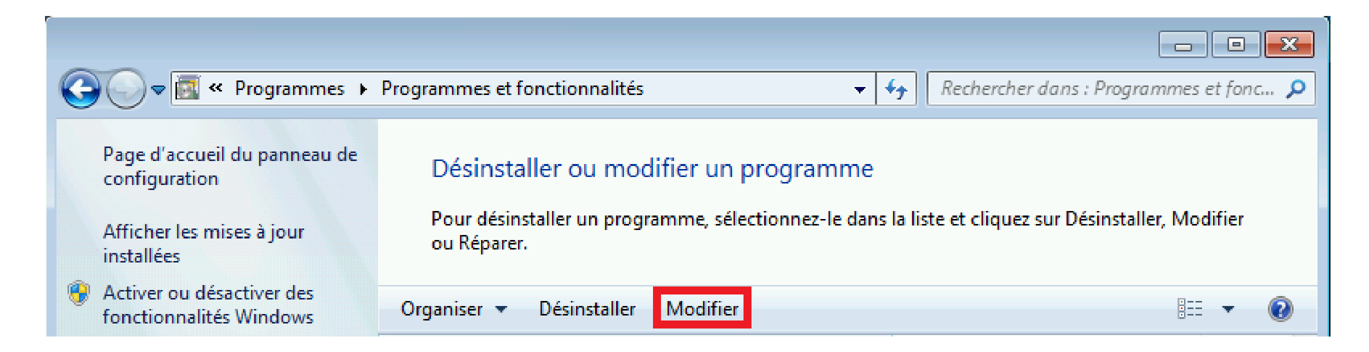
Si vous souhaitez ajouter ou supprimer des modules de l'installation actuelle, vous pouvez le faire sans devoir désinstaller Avira Antivirus Suite. Voici comment procéder :

- Modification d'une installation sous Windows 8
- Modification d'une installation sous Windows 7
- Modification d'une installation sous Windows XP

3.9.2 Modification d'une installation sous Windows 8

Vous avez la possibilité d'ajouter ou de supprimer certains composants de programme de l'installation actuelle de Avira Antivirus Suite (voir Sélection des composants d'installation).





Si vous souhaitez ajouter ou supprimer des composants de programme de l'installation actuelle, vous pouvez utiliser l'option **Désinstaller des programmes** dans le **Panneau de configuration Windows** pour **Modifier/Désinstaller** des programmes.

- Cliquez sur l'écran avec le bouton droit de la souris.

  L'icône **Toutes les applications** apparaît.

  Cliquez sur l'icône puis recherchez le **Panneau de configuration** dans la rubrique *Applications - système Windows*.

  Double-cliquez sur l'icône du **Panneau de configuration**.

  Cliquez sur **Programmes - désinstaller un programme**.

  Cliquez sur **Programmes et fonctionnalités - désinstaller un programme**.

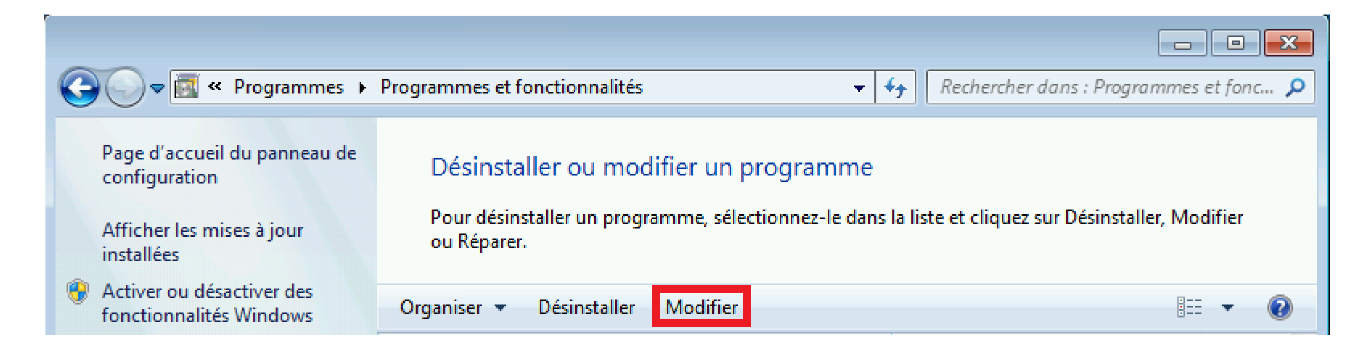
  Sélectionnez Avira Antivirus Suite puis cliquez sur **Modifier**.

  Dans la boîte de dialogue **Bienvenue** du programme, sélectionnez l'option **Modifier le programme**. Le système vous guide pas à pas pour procéder à la modification de l'installation.

Thèmes apparentés :
Sélection des composants d'installation

3.9.3 Modification d'une installation sous Windows 7

Vous avez la possibilité d'ajouter ou de supprimer certains composants de programme de l'installation actuelle de Avira Antivirus Suite (voir Sélection des composants d'installation).





Si vous souhaitez ajouter ou supprimer des composants de programme de l'installation actuelle, vous pouvez utiliser l'option **Programmes** dans le **Panneau de configuration Windows** pour **Modifier/Supprimer** des programmes.

- Ouvrez le **Panneau de configuration** via le menu **Démarrer** de Windows.

  Double-cliquez sur **Programmes et fonctionnalités**.

  Sélectionnez Avira Antivirus Suite puis cliquez sur **Modifier**.

  Dans la boîte de dialogue **Bienvenue** du programme, sélectionnez l'option **Modifier le programme**. Le système vous guide pas à pas pour procéder à la modification de l'installation.

Thèmes apparentés :
Sélection des composants d'installation

3.9.4 Modification d'une installation sous Windows XP

Vous avez la possibilité d'ajouter ou de supprimer certains composants de programme de l'installation actuelle de Avira Antivirus Suite (voir Sélection des modules d'installation).

Si vous souhaitez ajouter ou supprimer des composants de programme de l'installation actuelle, vous pouvez utiliser l'option **Programmes** dans le **Panneau de configuration Windows** pour **Modifier/Supprimer** des programmes.

- Ouvrez le **Panneau de configuration** via le menu **Démarrer > Paramètres** de Windows.

  Double-cliquez sur **Ajouter ou supprimer des programmes**.

  Sélectionnez Avira Antivirus Suite puis cliquez sur **Modifier**.

  Dans la boîte de dialogue **Bienvenue** du programme, sélectionnez l'option **Modifier le programme**. Le système vous guide pas à pas pour procéder à la modification de l'installation.

Thèmes apparentés :
Sélection des composants d'installation

3.10 Désinstallation d'Avira Antivirus Suite

3.10.1 Désinstallation de Avira Antivirus Suite

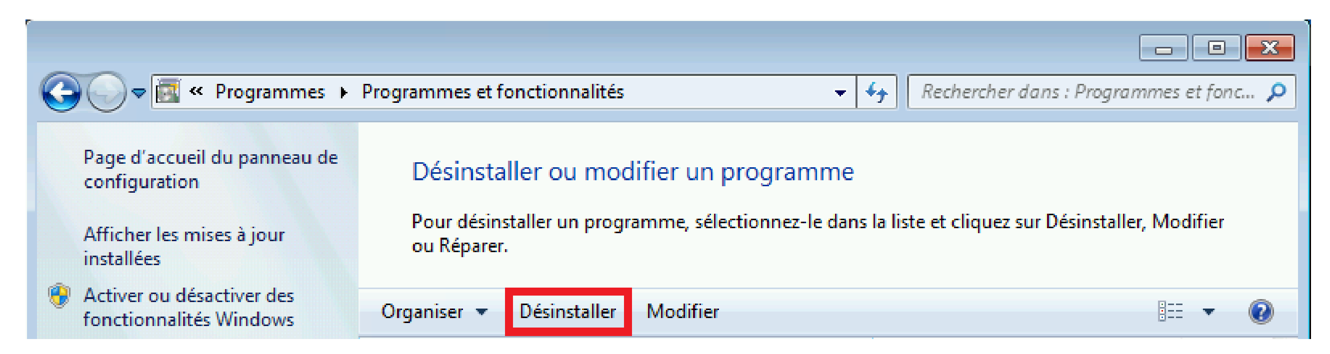
Si vous ressentiez le besoin de désinstaller Avira Antivirus Suite, voici comment procéder :

- Désinstallation de Avira Antivirus Suite sous Windows 8
- Désinstallation de Avira Antivirus Suite sous Windows 7
- Désinstallation de Avira Antivirus Suite sous Windows XP



3.10.2 Désinstallation de Avira Antivirus Suite sous Windows 8

Pour désinstaller Avira Antivirus Suite de votre ordinateur, utilisez l'option **Programmes et fonctionnalités** dans le panneau de configuration Windows.



- Cliquez sur l'écran avec le bouton droit de la souris.

  L'icône **Toutes les applications** apparaît.

  Cliquez sur l'icône puis recherchez le **Panneau de configuration** dans la rubrique *Applications - système Windows*.

  Double-cliquez sur l'icône du **Panneau de configuration**.

  Cliquez sur **Programmes - désinstaller un programme**.

  Cliquez sur **Programmes et fonctionnalités - désinstaller un programme**.

  Sélectionnez Avira Antivirus Suite dans la liste puis cliquez sur **Désinstaller**.

  Dans la demande de confirmation concernant la suppression de l'application et de tous ses composants, cliquez sur **Oui** pour confirmer.

  À la question de savoir si vous voulez activer le pare-feu Windows (Avira FireWall sera désinstallé), confirmez en cliquant sur **Oui** afin de conserver une protection minimale sur votre ordinateur.

  Tous les composants du programme sont supprimés.

  Cliquez sur **Terminer** pour terminer la désinstallation.

  Si une fenêtre de dialogue s'affiche en vous conseillant de redémarrer l'ordinateur, cliquez sur **Oui** pour confirmer.

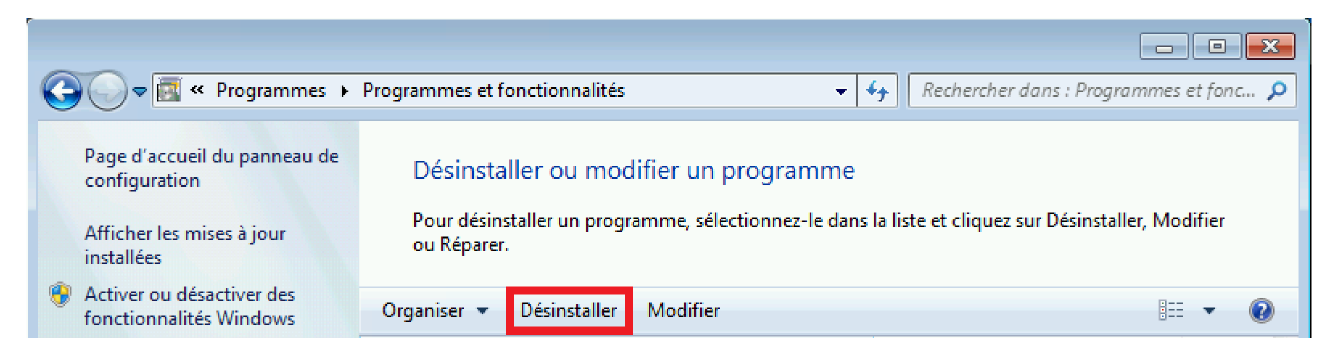
  Avira Antivirus Suite est maintenant désinstallé, votre ordinateur est redémarré si besoin est, et ce faisant, tous les répertoires, tous les fichiers et toutes les entrées de registre du programme sont supprimés.

> **Remarque**
> Avira SearchFree Toolbar n'est pas inclus dans le programme de désinstallation et doit être désinstallé à part.



3.10.3 Désinstallation de Avira Antivirus Suite sous Windows 7

Pour désinstaller Avira Antivirus Suite de votre ordinateur, utilisez l'option **Programmes et fonctionnalités** dans le panneau de configuration Windows.



- Ouvrez le **Panneau de configuration** via le menu **Démarrer** de Windows.

  Cliquez sur **Programmes et fonctionnalités**.

  Sélectionnez Avira Antivirus Suite dans la liste puis cliquez sur **Désinstaller**.

  Dans la demande de confirmation concernant la suppression de l'application et de tous ses composants, cliquez sur **Oui** pour confirmer.

  Si le programme vous demande si vous voulez activer le pare-feu Windows (Avira FireWall sera désinstallé), confirmez en cliquant sur **Oui** afin de conserver une protection minimale sur votre ordinateur.

  Tous les composants du programme sont supprimés.

  Cliquez sur **Terminer** pour terminer la désinstallation.

  Si une fenêtre de dialogue s'affiche en vous conseillant de redémarrer l'ordinateur, cliquez sur **Oui** pour confirmer.

  Avira Antivirus Suite est maintenant désinstallé, votre ordinateur est redémarré si besoin est, et ce faisant, tous les répertoires, tous les fichiers et toutes les entrées de registre du programme sont supprimés.

> **Remarque**
> Avira SearchFree Toolbar n'est pas inclus dans le programme de désinstallation et doit être désinstallé à part.

3.10.4 Désinstallation de Avira Antivirus Suite sous Windows XP

Pour désinstaller Avira Antivirus Suite de votre ordinateur, utilisez l'option **Modifier ou supprimer des programmes** dans le panneau de configuration Windows.

- Ouvrez le **Panneau de configuration** via le menu **Démarrer > Paramètres** de Windows.

  Double-cliquez sur **Ajouter ou supprimer des programmes**.

Sélectionnez Avira Antivirus Suite dans la liste puis cliquez sur **Supprimer**.

Dans la demande de confirmation concernant la suppression de l'application et de tous ses composants, cliquez sur **Oui** pour confirmer.

Tous les composants du programme sont supprimés.

Cliquez sur **Terminer** pour terminer la désinstallation.

Si une fenêtre de dialogue s'affiche en vous conseillant de redémarrer l'ordinateur, cliquez sur **Oui** pour confirmer.

Avira Antivirus Suite est maintenant désinstallé, votre ordinateur est redémarré si besoin est, et ce faisant, tous les répertoires, tous les fichiers et toutes les entrées de registre du programme sont supprimés.

> **Remarque**
> Avira SearchFree Toolbar n'est pas inclus dans le programme de désinstallation et doit être désinstallé à part.

3.10.5 Désinstallation d'Avira SearchFree Toolbar

Désinstallation de Avira SearchFree Toolbar

Si vous ressentiez le besoin de désinstaller Avira SearchFree Toolbar, voici comment procéder :

- Désinstallation de Avira SearchFree Toolbar sous Windows 8
- Désinstallation de Avira SearchFree Toolbar sous Windows 7
- Désinstallation de Avira SearchFree Toolbar sous Windows XP
- Désinstallation de Avira SearchFree Toolbar via le navigateur Internet
- Désinstallation de Avira SearchFree Toolbar via le gestionnaire de modules complémentaires

Désinstallation de Avira SearchFree Toolbar sous Windows 8

Pour désinstaller Avira SearchFree Toolbar :

- Fermez le navigateur Internet.

Cliquez sur un des coins inférieurs de l'écran avec le bouton droit de la souris.

L'icône **Toutes les applications** apparaît.

Cliquez sur l'icône puis recherchez le **Panneau de configuration** dans la rubrique *Applications - système Windows*.

Double-cliquez sur l'icône du **Panneau de configuration**.

Cliquez sur **Programmes - désinstaller un programme**.

Cliquez sur **Programmes et fonctionnalités - désinstaller un programme**.

Sélectionnez Avira SearchFree Toolbar plus Protection Web dans la liste et cliquez sur **Désinstaller**.

Un message vous demande alors si vous souhaitez vraiment désinstaller ce produit.

Confirmez en cliquant sur **Oui**.

Avira SearchFree Toolbar plus Protection Web sont désinstallés et tous les répertoires, fichiers ainsi que toutes les entrées de registre de Avira SearchFree Toolbar plus Protection Web sont supprimés au redémarrage de votre ordinateur.

Désinstallation de Avira SearchFree Toolbar sous Windows 7

Pour désinstaller Avira SearchFree Toolbar :

- Fermez votre navigateur Internet.

Ouvrez le **Panneau de configuration** via le menu **Démarrer** de Windows.

Double-cliquez sur **Programmes et fonctionnalités**.

Sélectionnez Avira SearchFree Toolbar plus Protection Web dans la liste et cliquez sur **Désinstaller**.

Un message vous demande alors si vous souhaitez vraiment désinstaller ce produit.

Confirmez en cliquant sur **Oui**.

Avira SearchFree Toolbar plus Protection Web sont désinstallés et tous les répertoires, fichiers ainsi que toutes les entrées de registre de Avira SearchFree Toolbar plus Protection Web sont supprimés au redémarrage de votre ordinateur.

Désinstallation de Avira SearchFree Toolbar sous Windows XP

Pour désinstaller Avira SearchFree Toolbar :

- Fermez votre navigateur Internet.

Ouvrez le **Panneau de configuration** via le menu **Démarrer > Paramètres** de Windows.

Double-cliquez sur **Ajouter ou supprimer des programmes**.

Sélectionnez Avira SearchFree Toolbar plus Protection Web dans la liste et cliquez sur **Supprimer**.

Un message vous demande alors si vous souhaitez vraiment désinstaller ce produit.

Confirmez en cliquant sur **Oui**.

Avira SearchFree Toolbar plus Protection Web sont désinstallés et tous les répertoires, fichiers ainsi que toutes les entrées de registre de Avira SearchFree Toolbar plus Protection Web sont supprimés au redémarrage de votre ordinateur.

Désinstallation de Avira SearchFree Toolbar via le navigateur Internet

Vous avez également la possibilité de désinstaller Avira SearchFree Toolbar directement dans le navigateur. Cette option est uniquement disponible pour Firefox et Internet Explorer :

- Ouvrez votre navigateur Internet.

  Ouvrez le menu **Options** dans la barre de recherche.

  Cliquez sur **Désinstaller la barre d'outils du navigateur**.

  Si le programme vous invite à installer le produit, confirmez en cliquant sur **Oui**.

  Le programme vous demande maintenant de fermer votre navigateur Internet.

  Fermez le navigateur Internet et cliquez sur **Réessayer**.

  Avira SearchFree Toolbar plus Protection Web sont désinstallés et tous les répertoires, fichiers ainsi que toutes les entrées de registre de Avira SearchFree Toolbar plus Protection Web sont supprimés au redémarrage de votre ordinateur.

> **Remarque**
> La barre d'outils doit être activée dans le gestionnaire des modules complémentaires pour désinstaller Avira SearchFree Toolbar.

Désinstallation de Avira SearchFree Toolbar via le gestionnaire de modules complémentaires

Étant donné que la barre d'outils est installée sous forme de module complémentaire, il est également possible de la désinstaller en tant que tel :

Firefox

- Cliquez sur **Outils > Modules complémentaires > Extensions**. Vous pouvez y gérer le module complémentaire Avira, c'est-à-dire activer ou désactiver la barre d'outils et la désinstaller.

Internet Explorer

- Cliquez sur **Gérer les modules complémentaires > Barres d'outils et extensions**. Vous pouvez alors activer, désactiver et désinstaller le module complémentaire Avira SearchFree Toolbar.

Google Chrome

- Le menu **Outils > Extensions** vous permet de gérer facilement votre barre d'outils, et donc de l'activer, la désactiver ou la désinstaller.



4. Aperçu d'Avira Antivirus Suite

Dans ce chapitre, vous obtenez une vue d'ensemble des fonctionnalités et de l'utilisation de votre produit Avira.

- voir chapitre Interface et utilisation
- voir chapitre Avira SearchFree Toolbar
- voir chapitre Comment procéder

4.1 Interface et utilisation

L'utilisation de votre produit Avira se fait via trois éléments d'interface du programme :

- Control Center : surveillance et gestion du produit Avira
- Configuration : configuration du produit Avira
- Icône de la barre d'état dans la zone de notification de la barre des tâches : ouverture du Control Center et d'autres fonctions

4.1.1 Control Center

Le Control Center sert à vérifier l'état de protection de votre ordinateur, à gérer et à utiliser les composants de protection et les fonctions de votre produit Avira.



La fenêtre du Control Center se divise en trois zones : la **barre de menu**, la **zone de navigation** et la fenêtre de détail **État** :

- **Barre de menu :** dans les menus du Control Center, vous pouvez accéder aux fonctions générales du programme et à des informations sur le produit.
- **Zone de navigation :** la zone de navigation vous permet de passer d'une rubrique à l'autre du Control Center. Les différentes rubriques contiennent des informations et fonctions des composants du programme et sont classées dans la barre de navigation selon les champs d'action. Exemple : champ d'action *SÉCURITÉ PC* - rubrique **Protection temps réel**.
- **État :** l'écran de démarrage **État** vous indique immédiatement si votre ordinateur est suffisamment protégé, ainsi que les modules actifs, la date de la dernière sauvegarde et le dernier contrôle du système. La fenêtre **État** comprend tous les boutons de fonctions ou d'actions, comme l'activation ou la désactivation de la **protection temps réel**.

Démarrage et arrêt du Control Center

Vous disposez des options suivantes pour démarrer le Control Center :

- Cliquez deux fois sur l'icône du programme sur le Bureau

- Via l'entrée de programme dans le menu **Démarrer > Programmes**.
- Via l'icône de la barre d'état de votre produit Avira.

Vous quittez le Control Center via la commande de menu **Quitter** dans le menu **Fichier**, avec la commande clavier **Alt+F4** ou en cliquant sur la croix de fermeture dans le Control Center.

Utilisation du Control Center

Voici comment naviguer dans le Control Center :

- Cliquez dans la barre de navigation sur un champ d'action sous une rubrique.
  - ↳ Le champ d'action apparaît avec les autres options de fonctions et de configuration dans la fenêtre de détail.
- Cliquez, le cas échéant, sur un autre champ pour les afficher dans la fenêtre de détail.

> **Remarque**
> La touche [**Alt**] permet d'activer la navigation au clavier dans la barre de menus. La touche **Entrée** vous permet d'activer la rubrique actuellement sélectionnée. Pour ouvrir et fermer des menus du Control Center, ou parcourir ceux-ci, vous pouvez également utiliser des raccourcis clavier : touche [**Alt**] + lettre soulignée du menu ou de la commande de menu. Maintenez la touche [**Alt**] enfoncée quand vous souhaitez accéder à une commande de menu ou à un sous-menu à partir du menu.

Voici comment traiter les données ou objets affichés dans la fenêtre de détail :

- Sélectionnez les données ou objets que vous souhaitez traiter.

  Pour sélectionner plusieurs éléments, maintenez la touche **Ctrl** ou **Maj** (sélection d'éléments situés les uns sous les autres) enfoncée pendant la sélection des éléments.
- Cliquez sur le bouton souhaité dans la barre supérieure de la fenêtre de détail pour traiter l'objet.

Aperçu du Control Center

- **État** : l'écran de démarrage **État** présente toutes les rubriques vous permettant de surveiller les fonctionnalités du programme (voir État).
  - La fenêtre **État** vous permet de voir d'un seul coup d'œil quels modules sont actifs et fournit des informations sur la dernière mise à jour effectuée.
- *SÉCURITÉ PC* : vous trouverez ici les composants vous permettant de contrôler l'absence de virus et de logiciels malveillants dans les fichiers de votre ordinateur.
  - La rubrique **Scanner** vous permet de configurer et de démarrer simplement la recherche directe (voir Scanner). Les profils prédéfinis permettent d'effectuer une

recherche avec des options standard adaptées. À l'aide de la sélection manuelle (qui est enregistrée) ou en créant des profils personnalisés, vous pouvez également adapter la recherche de virus et de programmes indésirables à vos besoins personnels.

- La rubrique Protection temps réel vous fournit des informations sur les fichiers contrôlés, ainsi que d'autres données statistiques, pouvant être réinitialisées à tout moment, et vous permet d'accéder au fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.

- *SÉCURITÉ INTERNET* : vous trouverez ici les composants vous permettant de protéger votre ordinateur contre les virus et logiciels malveillants provenant d'Internet et les accès réseau indésirables.
  - La rubrique **FireWall** vous permet de configurer les paramètres de base du FireWall. En outre, les débits actuels et toutes les applications actives utilisant une connexion réseau s'affichent (voir FireWall).
  - La rubrique Protection Web vous fournit des informations sur les URL contrôlées et les virus trouvés, ainsi que d'autres données statistiques qu'il est possible de réinitialiser à tout moment, et vous permet d'afficher le fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.
  - La rubrique **Protection e-mail** vous indique les e-mails contrôlés par ce service, leurs propriétés ainsi que d'autres données statistiques. (voir Protection e-mail).
- *PROTECTION MOBILE* : la catégorie Avira Free Android Security vous permet d'accéder en ligne à vos appareils Android.
  - Avira Free Android Security vous permet de gérer tous vos appareils dotés d'un système d'exploitation Android.
- *ADMINISTRATION* : vous trouverez ici des outils vous permettant d'isoler et de gérer les fichiers suspects ou infectés par des virus ainsi que de planifier des tâches récurrentes.
  - Sous la rubrique **Quarantaine** se trouve le gestionnaire de quarantaines. Il s'agit de l'emplacement central pour les fichiers déjà en quarantaine ou pour les fichiers suspects que vous souhaitez mettre en quarantaine (voir Quarantaine). En outre, vous avez la possibilité d'envoyer un fichier par e-mail à l'Avira Malware Research Center.
  - La rubrique **Planificateur** vous permet de créer des tâches de contrôle et de mise à jour programmées ainsi que des tâches de sauvegarde et d'adapter ou de supprimer les tâches existantes (voir Planificateur).
  - La rubrique **Rapports** vous permet de visualiser les résultats des actions effectuées (voir Rapports).
  - La rubrique **Événements** vous permet de vous informer sur les événements générés par les modules du programme (voir Événements).

4.1.2 Configuration

Dans la configuration, vous pouvez définir les paramètres de votre produit Avira. Après l'installation, votre produit Avira est configuré avec les paramètres par défaut qui garantissent une protection optimale de votre ordinateur. Toutefois, votre ordinateur ou vos exigences envers votre produit Avira peuvent présenter des particularités nécessitant l'ajustement de la configuration des composants de protection du programme.

La configuration se présente sous la forme d'une fenêtre de dialogue : les boutons **OK** ou **Appliquer** vous permettent d'enregistrer les paramètres définis dans la configuration, **Annuler** vous permet d'annuler vos paramètres et le bouton **Valeurs par défaut** vous permet de réinitialiser les paramètres de la configuration aux valeurs par défaut. Dans la barre de navigation à gauche, vous pouvez choisir les diverses rubriques de configuration.

Accès à la configuration

Vous avez plusieurs possibilités pour accéder à la configuration :

- Via le Panneau de configuration de Windows.
- Via le Centre de sécurité Windows - à partir de Windows XP Service Pack 2.
- Via l'icône de la barre d'état de votre programme Avira.
- Dans le Control Center via la rubrique Extras > Configuration.

- Dans le Control Center via le bouton Configuration.

> **Remarque**
> Si vous accédez à la configuration via le bouton **Configuration** du Control Center, vous arrivez dans le répertoire de configuration de la rubrique active dans le Control Center.

Gestion de la configuration

Vous naviguez dans la fenêtre de configuration comme dans l'explorateur Windows :

- Cliquez sur une entrée de l'arborescence pour afficher cette rubrique de configuration dans la fenêtre de détail.
- Cliquez sur le signe plus devant une entrée pour agrandir la rubrique de configuration et afficher les sous-rubriques de la configuration dans l'arborescence.
- Pour masquer les sous-rubriques de la configuration, cliquez sur le signe moins devant la rubrique de configuration agrandie.

> **Remarque**
> Pour activer ou désactiver des options dans la configuration et appuyer sur des boutons, vous pouvez également utiliser les raccourcis clavier : touche [**Alt**] + lettre soulignée dans le nom de l'option ou de la désignation du bouton.

Si vous souhaitez valider vos paramètres dans la configuration :

- Cliquez sur le bouton **OK**.

  ↳ La fenêtre de configuration se ferme et les paramètres sont validés.

  \- OU -

  Cliquez sur le bouton **Valider**.

  ↳ Les paramètres définis sont validés. La fenêtre de configuration reste ouverte.

Si vous souhaitez quitter la configuration sans valider vos paramètres :

- Cliquez sur le bouton **Annuler**.

  ↳ La fenêtre de configuration se ferme et les paramètres sont rejetés.

Si vous souhaitez réinitialiser tous les paramètres de la configuration aux valeurs par défaut :

- Cliquez sur **Valeurs par défaut**.

  ↳ Tous les paramètres de la configuration sont réinitialisés aux valeurs par défaut. Toutes les modifications et vos saisies sont perdues en cas de restauration des valeurs par défaut.

Aperçu des options de configuration

Vous disposez des options de configuration suivantes :

- **Scanner** : configuration de la recherche directe
  - Options de recherche
  - Action si résultat positif
  - Options pour la recherche dans les archives
  - Exceptions de la recherche directe
  - Heuristique de la recherche directe
  - Réglage de la fonction de rapport
- **Protection temps réel** : configuration de la recherche en temps réel
  - Options de recherche
  - Action si résultat positif
  - Autres actions
  - Exceptions de la recherche en temps réel
  - Heuristique de la recherche en temps réel
  - Réglage de la fonction de rapport
- **Mise à jour** : configurations des paramètres de mise à jour
  - Télécharger via le serveur Web
- **Protection Web** : configuration de la protection Web
  - Options de recherche, activation et désactivation de la protection Web
  - Action si résultat positif
  - Accès bloqués : types de fichiers et types MIME indésirables, filtre Web pour les URL connues indésirables (logiciels malveillants, hameçonnage, etc.)
  - Exceptions de recherche de la protection Web : URL, types de fichiers, types MIME
  - Heuristique de la protection Web
  - Réglage de la fonction de rapport
- **Protection e-mail** : configuration de la protection e-mail
  - Options de recherche : activation de la surveillance des comptes POP3, des comptes IMAP, des e-mails sortants (SMTP)
  - Action si résultat positif
  - Autres actions
  - Heuristique de la recherche de la protection e-mail
  - Exceptions de la recherche de la protection e-mail
  - Configuration de la mémoire tampon, vider la mémoire tampon
  - Réglage de la fonction de rapport
- **Généralités** :
  - Catégories étendues de dangers pour la recherche directe et en temps réel
  - Protection étendue : activer ProActiv et la protection Cloud

- Filtre des applications : bloquer ou autoriser des applications
- Protection par mot de passe pour l'accès au Control Center et à la configuration
- Sécurité : bloquer les fonctions Autorun, verrouiller les fichiers hôtes Windows, protection du produit
- WMI : activer la prise en charge WMI
- Configuration de la consignation des événements
- Configuration des fonctions de rapport
- Réglage des répertoires utilisés
- Configuration des avertissements sonores en cas de détection de logiciel malveillant

4.1.3 Icône de la barre d'état

Après l'installation, l'icône de barre d'état de votre produit Avira s'affiche dans la zone de notification de la barre des tâches :

Icône	Description
	La protection temps réel Avira est activée
	La protection temps réel Avira est désactivée

L'icône dans la barre des tâches affiche l'état de la Protection temps réel .

Les fonctions centrales de votre produit Avira sont rapidement accessibles via le menu contextuel de l'icône de la barre d'état.

- Pour accéder au menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de la barre d'état.

Entrées dans le menu contextuel

- **Activer la protection temps réel** : active ou désactive la protection temps réel Avira.
- **Activer la protection e-mail** : active ou désactive la protection e-mail Avira.
- **Activer la protection Web** : active ou désactive la protection Web Avira.
  - **Activer Pare-feu Windows** : active ou désactive Pare-feu Windows (cette fonction est disponible à partir de Windows 8 seulement).
- **Démarrer Avira Antivirus Suite** : ouvre le Control Center.
- **Configurer Avira Antivirus Suite : ouvre la configuration.**
- **Mes messages : ouvre un message-bannière avec les derniers messages concernant votre produit Avira.**

- **Mes paramètres de communication : ouvre le centre d'abonnement pour les notifications produits**
- **Démarrer mise à jour : démarre une mise à jour.**
- **Aide : ouvre l'aide en ligne.**
- **À propos de Avira Antivirus Suite : ouvre une boîte de dialogue avec des informations sur votre produit Avira : informations sur le produit, la version, la licence.**
- **Avira sur Internet : ouvre le portail Web Avira sur Internet. Un accès Internet est nécessaire.**

4.2 Avira SearchFree Toolbar

L'Avira SearchFree Toolbar comprend deux principaux composants : Avira SearchFree et la barre d'outils.

La nouvelle Avira SearchFree Toolbar s'installe sous la forme de module complémentaire. Lorsque vous accédez la première fois au navigateur (Internet Explorer ou Firefox), un message vous demande si vous acceptez que le programme de l'Avira SearchFree Toolbar modifie votre navigateur. Vous devez accepter afin de garantir le succès de l'installation de l'Avira SearchFree Toolbar.

Avira SearchFree est le nouveau moteur de recherche d'Avira et contient un logo Avira sur lequel vous pouvez cliquer pour être redirigé vers le site Web d'Avira, ainsi que des canaux Web et d'images. Il permet aux utilisateurs d'Avira d'effectuer une recherche complète et plus sûre.

La barre d'outils est intégrée à votre navigateur Web et comprend un champ de recherche, un logo Avira redirigeant vers le site Web d'Avira, deux affichages d'état, trois widgets et le menu **Options**.

- Barre de recherche
  Utilisez la barre de recherche pour naviguer sur Internet rapidement et gratuitement à l'aide du moteur de recherche Avira SearchFree.
- Affichage d'état
  Les affichages d'état décrivent l'état de la protection Web et le statut de mise à jour actuel de votre produit Avira, et vous permettent d'identifier les actions à entreprendre pour protéger votre PC.
- Widgets
  Avira vous permet d'accéder directement aux fonctions importantes sur Internet, par exemple vos messages Facebook ou votre messagerie. Vous pouvez également définir la protection de votre système grâce au widget Protection Web (uniquement sur Firefox et Internet Explorer).
- Options
  Le menu Options vous permet d'accéder aux options de Toolbar, d'effacer l'historique de recherche, de consulter l'aide et les informations concernant la barre d'outils et de

désinstaller l'Avira SearchFree Toolbar directement à partir du navigateur Web (Firefox et Internet Explorer uniquement).

4.2.1 Utilisation

Barre de recherche

La barre de recherche vous permet de rechercher un ou plusieurs termes sur Internet.

Saisissez à cet effet le terme dans le champ de recherche et cliquez sur la touche **Entrée** ou cliquez sur **Recherche**. L'outil de recherche Avira SearchFree parcourt Internet pour vous et affiche tous les résultats dans la fenêtre du navigateur.

Vous pouvez configurer Avira SearchFree à votre guise dans **Options** sur Internet Explorer, Firefox et Chrome.

Affichage d'état

Protection Web

Pour déterminer l'état de sécurité de votre ordinateur, vous pouvez utiliser les icônes et messages suivants :

Icône	Affichage d'état	Description
✓	*Protection Web*	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : *La Protection Web d'Avira est activée. Votre navigation est securisée.* Aucune autre action n'est donc requise.
!	*Protection Web désactivée*	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : *La Protection Web d'Avira est désactivée. Cliquez ici pour découvrir comment l'activer.* ↳ Vous êtes redirigé vers un article de notre base de connaissances.



	Protection Web non installée	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : • *La Protection Web d'Avira n'est pas installée sur cet appareil. Cliquez ici pour découvrir comment sécuriser votre navigation.* Cela signifie que vous avez désinstallé l'antivirus Avira ou qu'il n'est pas installé correctement. • *Avec Avira Antivirus, vous bénéficiez gratuitement de Protection Web. Cliquez ici pour découvrir comment l'installer.* Cela signifie que vous n'avez pas installé la protection Web ou que vous l'avez désinstallée. ↳ Dans les deux cas, vous êtes redirigé sur la page Web d'Avira sur laquelle vous pouvez télécharger votre produit Avira.
	Erreur	Si vous déplacez le curseur de la souris sur l'icône, le message suivant s'affiche : *Avira a signalé une erreur.* ▸ Cliquez sur l'icône grise ou sur le texte pour accéder à la page de support Avira.

Widgets

L'Avira SearchFree Toolbar dispose de 3 widgets avec les principales fonctions d'Internet : Facebook, messagerie électronique et protection Web.

Facebook

Cette fonction vous permet de recevoir directement les messages Facebook et donc de rester toujours au courant.

E-mail

Si vous cliquez sur l'icône e-mail, une liste déroulante s'affiche et vous permet de sélectionner parmi les principales messageries.



Protection Web

Ce widget a été développé par Avira et permet d'accéder très simplement à toutes les options de sécurité Internet. Pour le moment, il n'est disponible qu'avec Firefox et Internet Explorer. Différentes options sont proposées, elles peuvent porter des noms différents selon le navigateur :

- *Blocage des pop-up*

Si cette option est activée, toutes les fenêtres pop-up sont bloquées lorsque vous naviguez sur Internet.

- *Blocage des cookies*

Si cette option est activée, aucun cookie n'est enregistré pendant la navigation.

- *Mode privé (Firefox) / Navigation InPrivate (Internet Explorer)*

Si cette option est activée, vous ne laissez aucune trace lorsque vous naviguez sur Internet. Cette option n'est pas disponible pour Internet Explorer 7 et 8.

- *Supprimer l'historique récent (Firefox) / Supprimer l'historique de navigation (Internet Explorer)*

Cette option vous permet de supprimer toutes les activités Internet actuelles.

Conseiller en sécurité

Le conseiller en sécurité vous propose des niveaux de sécurité pendant que vous naviguez sur Internet.
Vous pouvez ainsi évaluer si le site que vous consultez présente un risque élevé ou faible pour votre sécurité.
Ce widget vous fournit des informations concernant le site Internet, comme le propriétaire du domaine, ou la raison du niveau de sécurité.
On compte trois niveaux de sécurité : sûr, peu risqué et très risqué.

Les niveaux de sécurité s'affichent dans la barre d'outils et dans les résultats de recherche sous la forme d'une icône de barre d'état Avira avec différents symboles :

Icône	Affichage d'état	Description
	Sûr	Une coche verte pour les sites Internet les plus sûrs.
	Risqué faible	Un point d'exclamation jaune pour les sites Internet qui présentent un risque faible.

	Risque élevé	Un panneau stop rouge pour les sites Internet présentant un risque élevé pour votre sécurité.
	Manqué	Un point d'interrogation gris pour les sites Internet dont le risque ne peut être évalué.
	Vérifier	Ce symbole s'affiche pendant la vérification de l'état.

Bloqueur de suivi

Le bloqueur de suivi vous permet d'interrompre le suivi et d'empêcher toute collecte d'informations lorsque vous naviguez sur Internet.
Le widget vous permet de sélectionner le suivi à bloquer et à autoriser.

Les entreprises se divisent en trois catégories :

- Réseaux sociaux
- Réseaux
- Autres entreprises

4.2.2 Options

L'Avira SearchFree Toolbar est compatible avec Internet Explorer, Firefox et Google Chrome, et peut être configurée à votre gré dans les navigateurs Web :

- Options de configuration Internet Explorer
- Options de configuration Firefox
- Options de configuration Chrome

Internet Explorer

Dans le navigateur Internet Explorer, vous disposez des options de configuration suivantes pour l'Avira SearchFree Toolbar dans le menu **Options** :

Options de Toolbar

Recherche

Sélectionner moteur Avira

Dans le menu **Sélectionner moteur Avira**, vous pouvez sélectionner le moteur de recherche à utiliser pour les recherches. Vous avez le choix entre des moteurs de recherche de différents pays : États-Unis, Brésil, Allemagne, Espagne, Europe, France, Italie, Pays-Bas, Russie et Grande-Bretagne.

Ouvrir recherches dans

Dans le menu de l'option **Ouvrir recherches dans**, vous pouvez sélectionner où afficher le résultat de la recherche, dans la **Fenêtre actuelle**, dans une **Nouvelle fenêtre** ou dans un **Nouvel onglet**.

Afficher les recherches récentes

Si l'option **Afficher les recherches récentes** est activée, vous pouvez demander l'affichage des termes saisis jusqu'alors sous le champ de saisie de la barre de recherche.

Supprimer historique des recherches en quittant le navigateur

Activez l'option **Supprimer historique des recherches en quittant le navigateur** si vous ne souhaitez pas enregistrer l'historique des recherches déjà effectuées mais si vous préférez les effacer lors de la fermeture du navigateur Web.

Autres options

Langue de Toolbar

Sous **Langue de Toolbar**, vous pouvez sélectionner la langue d'affichage de l'Avira SearchFree Toolbar. Vous avez le choix entre l'anglais, l'allemand, l'espagnol, le français, l'italien, le portugais et le néerlandais.

> **Remarque**
> La langue prédéfinie de l'Avira SearchFree Toolbar correspond à celle de votre programme, si elle est disponible. Si la barre d'outils n'est pas disponible dans votre langue, l'anglais est défini par défaut.

Afficher le texte des boutons

Désactivez l'option **Afficher le texte des boutons** si vous souhaitez masquer le texte à côté des icônes de l'Avira SearchFree Toolbar.

Supprimer l'historique

Activez l'option **Supprimer l'historique**, si vous ne souhaitez pas enregistrer la/les recherche(s) déjà effectué(es) mais préférez la/les supprimer immédiatement.

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Désinstaller

Vous pouvez également désinstaller directement l'Avira SearchFree Toolbar sur Internet Explorer : Désinstallation de Avira SearchFree Toolbar via le navigateur Internet.



A propos

Cliquez sur **A propos** pour afficher la version de l'Avira SearchFree Toolbar installée.

Firefox

Dans le navigateur Firefox, vous disposez des options de configuration suivantes pour l'Avira SearchFree Toolbar dans le menu **Options** :

Options de Toolbar

Recherche

Sélectionner moteur Avira

Dans le menu **Sélectionner moteur Avira**, vous pouvez sélectionner le moteur de recherche à utiliser pour les recherches. Vous avez le choix entre des moteurs de recherche de différents pays : États-Unis, Brésil, Allemagne, Espagne, Europe, France, Italie, Pays-Bas, Russie et Grande-Bretagne.

Afficher les recherches récentes

Si l'option **Afficher les recherches récentes** est activée, vous pouvez demander l'affichage des termes saisis jusqu'alors en cliquant sur la flèche dans la barre de recherche. Sélectionnez l'un des termes si vous souhaitez afficher de nouveau les résultats de recherche.

Supprimer historique des recherches en quittant le navigateur

Activez l'option **Supprimer historique des recherches en quittant le navigateur** si vous ne souhaitez pas enregistrer l'historique des recherches déjà effectuées mais si vous préférez les effacer lors de la fermeture du navigateur Web.

Afficher les résultats de recherches d'Ask lorsque je tape des mots-clés ou des URL non valides dans la barre d'adresse du navigateur

Si cette option est activée, chaque fois que vous saisissez des mots-clés ou une adresse URL non valide dans le champ d'adresse du navigateur Web, une recherche est lancée et les résultats s'affichent.

Autres options

Langue de Toolbar

Sous **Langue de Toolbar**, vous pouvez sélectionner la langue d'affichage de l'Avira SearchFree Toolbar. Vous avez le choix entre l'anglais, l'allemand, l'espagnol, le français, l'italien, le portugais et le néerlandais.

Remarque
La langue prédéfinie de l'Avira SearchFree Toolbar correspond à celle de votre programme, si elle est disponible. Si la barre d'outils n'est pas disponible dans votre langue, l'anglais est défini par défaut.

Afficher le texte des boutons

Désactivez l'option **Afficher le texte des boutons** si vous souhaitez masquer le texte à côté des icônes de l'Avira SearchFree Toolbar.

Supprimer l'historique

Activez l'option **Supprimer l'historique**, si vous ne souhaitez pas enregistrer la/les recherche(s) déjà effectué(es) mais préférez la/les supprimer immédiatement.

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Désinstaller

Vous pouvez également désinstaller directement l'Avira SearchFree Toolbar sur Internet Explorer : Désinstallation via le navigateur Web.

A propos

Cliquez sur **A propos** pour afficher la version de l'Avira SearchFree Toolbar installée.

Chrome

Toutes les options de configuration sous le parapluie rouge Avira se trouvent dans le navigateur Web Google Chrome. Vous disposez des options suivantes pour l'Avira SearchFree Toolbar :

Aide

Cliquez sur **Aide** pour accéder au site Web et aux questions fréquentes (FAQ) sur la barre d'outils.

Instructions de désinstallation

Des liens vers les instructions de désinstallation de l'Avira SearchFree Toolbar sont disponibles ici.

A propos

Cliquez sur **A propos** pour afficher la version de l'Avira SearchFree Toolbar installée.

Afficher et masquer l'Avira SearchFree Toolbar

Cette option de menu permet de masquer et d'afficher l'Avira SearchFree Toolbar qui se trouve dans la partie supérieure de la fenêtre.

4.2.3 Désinstallation de Avira SearchFree Toolbar sous Windows 7

Pour désinstaller Avira SearchFree Toolbar :

- Fermez votre navigateur Internet.

  Ouvrez le **Panneau de configuration** via le menu **Démarrer** de Windows.

  Double-cliquez sur **Programmes et fonctionnalités**.

  Sélectionnez Avira SearchFree Toolbar plus Protection Web dans la liste et cliquez sur **Désinstaller**.

  Un message vous demande alors si vous souhaitez vraiment désinstaller ce produit.

  Confirmez en cliquant sur **Oui**.

  Avira SearchFree Toolbar plus Protection Web sont désinstallés et tous les répertoires, fichiers ainsi que toutes les entrées de registre de Avira SearchFree Toolbar plus Protection Web sont supprimés au redémarrage de votre ordinateur.

4.3 Comment procéder

Les chapitres « Comment procéder » vous fournissent une rapide description de la procédure d'activation de la licence et du produit ainsi que des principales fonctions de votre produit Avira. Les courts descriptifs sélectionnés vous permettent d'obtenir rapidement un aperçu des fonctionnalités de votre produit Avira. Ils ne remplacent toutefois pas les explications détaillées fournies dans les différents chapitres de cette Aide.

4.3.1 Activer licence

Pour activer la licence de votre produit Avira, procédez de la manière suivante :

Avec le fichier de licence *.KEY*, vous activez votre licence pour votre produit Avira. Vous recevez votre fichier de licence par e-mail. Le fichier de licence contient la licence pour tous les produits que vous avez commandés.

Si vous n'avez pas encore installé votre produit Avira :

- Enregistrez le fichier de licence dans un répertoire local de votre ordinateur.
- Installez votre produit Avira.
- Lors de l'installation, indiquez où vous avez enregistré le fichier de licence.

Si vous avez déjà installé votre produit Avira :

- Double-cliquez dans votre gestionnaire de fichiers ou dans l'e-mail d'activation sur le fichier de licence et suivez les instructions à l'écran du gestionnaire de licences qui s'affiche.

  \- OU -

Dans le Control Center de votre produit Avira, sélectionnez l'entrée de menu **Aide > Gestion des licences**.

> **Remarque**
> Sous Windows Vista, la fenêtre de dialogue Contrôle de compte d'utilisateur apparaît. Connectez-vous comme administrateur le cas échéant. Cliquez sur **Continuer**.

- Sélectionnez le fichier de licence et cliquez sur **Ouvrir**.
  - ↳ Un message s'affiche.
- Validez avec **OK**.
  - ↳ La licence est activée.
- Redémarrez le système si nécessaire.

4.3.2 Activer le produit

Pour activer votre produit Avira, vous disposez des options suivantes :

- Activation avec une licence complète valide

  Pour activer le programme avec une licence complète, vous avez besoin d'un code d'activation valide, par le biais duquel les données de votre licence sont enregistrées. Soit nous vous avons envoyé le code d'activation par e-mail, soit celui-ci est indiqué sur l'emballage du produit.
- Activation avec une licence d'évaluation

  Votre produit Avira est activé par une licence d'évaluation générée automatiquement, grâce à laquelle vous pouvez tester l'intégralité des fonctions de votre produit Avira pendant une période limitée.

> **Remarque**
> Vous avez besoin d'une connexion Internet active pour activer le produit ou demander une licence test.
> Si aucune connexion ne peut être établie avec les serveurs Avira, vérifiez le cas échéant les paramètres du pare-feu utilisé : lors de l'activation du produit, les connexions sont établies via le protocole HTTP et le port 80 (communication) et via le protocole de cryptage SSL et le port 443. Assurez-vous que votre pare-feu ne bloque pas les données entrantes et sortantes. Vérifiez ensuite que vous pouvez accéder à des sites Internet par le biais de votre navigateur Web.

Pour activer votre produit Avira, procédez de la façon suivante :

Si vous n'avez pas encore installé votre produit Avira :

- Installez votre produit Avira.

↳ Au cours de l'installation, vous êtes invité à choisir une option d'activation.

- **Activer le produit** = activation avec une licence complète valide
- **Tester le produit** = activation avec une licence d'évaluation

- Indiquez le code d'activation dans le cas d'une activation avec licence complète.
- Confirmez la sélection du processus d'activation en cliquant sur **Suivant**.
- Entrez vos données personnelles pour vous inscrire, le cas échéant, et confirmez votre saisie en cliquant sur **Suivant**.

  ↳ Vos données de licence s'affichent dans la fenêtre de dialogue suivante. Votre produit Avira est activé.

- Poursuivez l'installation.

Si vous avez déjà installé votre produit Avira :

- Dans le Control Center, sélectionnez la rubrique **Aide > Gestion des licences**.

  ↳ L'assistant de licence s'affiche, dans lequel vous pouvez choisir une option d'activation. Les étapes suivantes de l'activation du produit sont identiques à celles de la procédure présentée ci-avant.

4.3.3 Effectuer des mises à jour automatiques

Pour créer une tâche de mise à jour automatique de votre produit Avira avec le planificateur Avira, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Planificateur**.
- Cliquez sur l'icône [+] **Créer une nouvelle tâche avec l'assistant**.

  ↳ La boîte de dialogue **Nom et description de la tâche** s'affiche.

- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.

  ↳ La boîte de dialogue **Type de tâche** s'affiche.

- Sélectionnez **Tâche de mise à jour** dans la liste de sélection.
- Cliquez sur **Suivant**.

  ↳ La boîte de dialogue **Heure de la tâche** s'affiche.

- Sélectionnez quand la mise à jour doit être effectuée :

- **Immédiatement**
- **Tous les jours**
- **Toutes les semaines**
- **Par intervalle**
- **Une fois**
- **Connexion**

> **Remarque**
> Nous vous recommandons d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 2 heures.

- Le cas échéant, saisissez la date selon votre sélection.
- Le cas échéant, sélectionnez des options supplémentaires (disponibles en fonction du type de tâche) :

- **Rattraper la tâche quand la date est déjà passée**
  Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- **Démarrer également la tâche quand une connexion Internet est établie**
  Outre la fréquence définie, la tâche est exécutée à chaque démarrage d'une connexion Internet.

- Cliquez sur **Suivant**.
  ↳ La boîte de dialogue **Affichage de la fenêtre** s'affiche.
- Sélectionnez le mode d'affichage de la fenêtre des tâches :

- **Invisible** : pas de fenêtre des tâches
- **Réduit** : uniquement la barre de progression
- **Agrandi** : fenêtre des tâches complète

- Cliquez sur **Terminer**.
  ↳ La tâche que vous venez de créer apparaît comme activée (cochée) sur l'écran principal de la rubrique *ADMINISTRATION* **> Planificateur**.
- Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

Les icônes suivantes vous permettent de continuer à modifier les tâches :

Afficher les propriétés d'une tâche

Modifier la tâche

Supprimer la tâche

Démarrer la tâche

Arrêter la tâche

4.3.4 Démarrer manuellement une mise à jour

Vous avez différentes possibilités de démarrer manuellement une mise à jour : une mise à jour du fichier de définitions des virus et du moteur de recherche est effectuée systématiquement dans le cas d'une mise à jour lancée manuellement.

Pour démarrer manuellement la mise à jour de votre produit Avira, procédez de la façon suivante :

- Avec le bouton droit de la souris, cliquez sur l'icône de la barre d'état Avira dans la barre des tâches et sélectionnez **Démarrer mise à jour**.

  \- OU -

- Dans le Control Center, sélectionnez la rubrique **État**, puis cliquez dans la zone **Dernière mise à jour** sur le lien **Démarrer mise à jour**.

  \- OU -

  Dans le menu **Mise à jour** du Control Center, sélectionnez la rubrique **Démarrer mise à jour**.

  ↳ La boîte de dialogue **Updater** s'affiche.

Remarque
Nous vous recommandons d'effectuer des mises à jour régulières. L'intervalle de mise à jour recommandé est : 2 heures.

Remarque
Vous pouvez également effectuer une mise à jour manuelle directement à partir du centre de sécurité Windows.

4.3.5 Recherche directe : chercher des virus et logiciels malveillants avec un profil de recherche

Un profil de recherche est un regroupement de lecteurs et répertoires à parcourir.

Pour rechercher via un profil de recherche, vous disposez des possibilités suivantes :

Utiliser un profil de recherche prédéfini

Si les profils de recherche prédéfinis répondent à vos besoins.

Adapter et utiliser un profil de recherche (sélection manuelle)

Si vous souhaitez chercher avec un profil de recherche individualisé.

Créer et utiliser un nouveau profil de recherche

Si vous souhaitez créer votre propre profil de recherche.

Selon le système d'exploitation, différentes icônes sont disponibles pour le démarrage d'un profil de recherche :

- Sous Windows XP :

  Cette icône vous permet de lancer la recherche via un profil de recherche.

- Sous Windows Vista :

  Sous Microsoft Windows Vista, le Control Center n'a pour le moment que des droits restreints (par exemple, pour l'accès aux répertoires et aux fichiers). Le Control Center ne peut exécuter certaines actions et accéder aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.

  - À l'aide de cette icône, vous démarrez une recherche limitée via un profil de recherche. Seuls les répertoires et fichiers pour lesquels le système d'exploitation a attribué les droits d'accès sont parcourus.
  - À l'aide de cette icône, vous démarrez la recherche avec des droits d'administrateur étendus. Après confirmation, tous les répertoires et fichiers dans le profil de recherche sélectionné sont parcourus.

Pour chercher des virus et logiciels malveillants avec un profil de recherche, procédez de la façon suivante :

- Dans le Control Center, choisissez la rubrique *SÉCURITÉ PC* **> Scanner**.

  ↳ Les profils de recherche prédéfinis s'affichent.

- Sélectionnez l'un des profils de recherche prédéfinis.

  -OU-

  Adaptez le profil de recherche **Sélection manuelle**.

  -OU-

  Créez un nouveau profil de recherche.

- Cliquez sur l'icône (Windows XP ou Windows Vista).
- La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.

  ↳ À la fin du processus de recherche, les résultats s'affichent.

Si vous souhaitez adapter un profil de recherche :

- Dans le profil de recherche **Sélection manuelle**, déployez l'arborescence des fichiers de façon à ouvrir tous les lecteurs et les répertoires devant être parcourus.
  - Cliquez sur le caractère **+** : le niveau de répertoire suivant s'affiche.

- Cliquez sur le caractère **-** : le niveau de répertoire suivant est masqué.
- Sélectionnez les nœuds et répertoires à scanner en cliquant sur la case correspondante pour le niveau de répertoire concerné :

  Pour sélectionner les répertoires, vous disposez des possibilités suivantes :

- Répertoire avec ses sous-répertoires (coche noire)
- Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
- Aucun répertoire (pas de coche)

Si vous souhaitez créer un profil de recherche :

- Cliquez sur l'icône **Créer un nouveau profil.**
  - ↳ Le profil **Nouveau profil** apparaît sous les profils existants.
- Renommez le profil de recherche si nécessaire, en cliquant sur l'icône .
- Sélectionnez les nœuds et répertoires à contrôler en cliquant une fois dans la case du niveau de répertoire concerné.

  Pour sélectionner les répertoires, vous disposez des possibilités suivantes :

- Répertoire avec ses sous-répertoires (coche noire)
- Uniquement les sous-répertoires d'un répertoire (coche grise, les sous-répertoires ont une coche noire)
- Aucun répertoire (pas de coche)

4.3.6 Recherche directe : chercher des virus et logiciels malveillants par glisser-déplacer

Pour chercher des virus et logiciels malveillants de manière ciblée par glisser-déplacer, procédez de la manière suivante :

- ✓ Ouvrez le Control Center de votre programme Avira.
- Sélectionnez le fichier ou le répertoire, qui doit être contrôlé.
- Avec le bouton gauche de la souris, faites glisser le fichier ou le répertoire sélectionné dans le Control Center.
  - ↳ La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.
  - ↳ À la fin du processus de recherche, les résultats s'affichent.

4.3.7 Recherche directe : chercher des virus et logiciels malveillants via le menu contextuel

Pour rechercher des virus et des logiciels malveillants de manière ciblée via le menu contextuel, procédez de la façon suivante :

- Cliquez (par ex. dans l'explorateur Windows, sur le Bureau ou dans un répertoire Windows ouvert) avec le bouton droit de la souris sur le fichier ou le répertoire, que vous souhaitez contrôler.
  - ↳ Le menu contextuel de l'explorateur Windows s'affiche.
- Dans le menu contextuel, sélectionnez **Contrôler les fichiers sélectionnés avec Avira**.
  - ↳ La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.
  - ↳ À la fin du processus de recherche, les résultats s'affichent.

4.3.8 Recherche directe : recherche automatisée de virus et logiciels malveillants

> **Remarque**
> Après l'installation, la tâche de contrôle *Contrôle intégral du système* est créée dans le planificateur : un contrôle intégral du système est effectué dans l'intervalle recommandé.

Pour créer une tâche de recherche automatisée des virus et logiciels malveillants, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Planificateur**.
- Cliquez sur l'icône + **Créer une nouvelle tâche avec l'assistant**.
  - ↳ La boîte de dialogue **Nom et description de la tâche** s'affiche.
- Nommez la tâche et décrivez-la si besoin est.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Type de tâche** s'affiche.
- Sélectionnez la **tâche de contrôle**.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Sélection du profil** s'affiche.
- Choisissez le profil qui doit être parcouru.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Heure de la tâche** s'affiche.
- Sélectionnez quand la recherche doit être effectuée :

- **Immédiatement**
- **Tous les jours**
- **Toutes les semaines**
- **Par intervalle**
- **Une fois**

- **Connexion**
- Le cas échéant, saisissez la date selon votre sélection.
- Sélectionnez l'option complémentaire le cas échéant (uniquement disponible en fonction du type de tâche) : **Rattraper la tâche quand la date est déjà passée**
  - ↳ Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
- Cliquez sur **Suivant**.
  - ↳ La boîte de dialogue **Affichage de la fenêtre** s'affiche.
- Sélectionnez le mode d'affichage de la fenêtre des tâches :
- **Invisible** : pas de fenêtre des tâches
- **Réduit** : uniquement la barre de progression
- **Agrandi** : fenêtre des tâches complète
- Sélectionnez l'option **Arrêter l'ordinateur quand la tâche a été exécutée**, si vous souhaitez que l'ordinateur s'arrête automatiquement dès que la tâche est exécutée et terminée.

  L'option est disponible uniquement en mode d'affichage de la fenêtre agrandi ou réduit.
- Cliquez sur **Terminer**.
  - ↳ La tâche que vous venez de créer apparaît comme activée (cochée) sur l'écran principal de la rubrique *ADMINISTRATION* **> Planificateur**.
- Désactivez éventuellement les tâches qui ne doivent pas être exécutées.

Les icônes suivantes vous permettent de continuer à modifier les tâches :

Afficher les propriétés d'une tâche

Modifier la tâche

Supprimer la tâche

Démarrer la tâche

Arrêter la tâche

4.3.9 Recherche directe : chercher les rootkits actifs de manière ciblée

Pour rechercher les rootkits actifs, utilisez le profil de recherche prédéfini **Recherche des rootkits et des logiciels malveillants actifs**.



Pour rechercher les rootkits actifs de manière ciblée, procédez de la façon suivante :

- Dans le Control Center, choisissez la rubrique *SÉCURITÉ PC* **> Scanner**.
  ↳ Les profils de recherche prédéfinis s'affichent.
- Sélectionnez le profil de recherche prédéfini **Recherche des rootkits et des logiciels malveillants actifs**.
- Sélectionnez les éventuels autres nœuds et répertoires à contrôler en cliquant dans la case du niveau de répertoire concerné.
- Cliquez sur l'icône (Windows XP ou Windows Vista).
  ↳ La fenêtre **Luke Filewalker** s'affiche et la recherche directe démarre.
  ↳ À la fin du processus de recherche, les résultats s'affichent.

4.3.10 Réagir aux virus et logiciels malveillants détectés

Pour les différents composants de protection de votre produit Avira, vous pouvez régler sous la rubrique **Action si résultat positif** la façon dont votre produit Avira doit réagir en cas de détection d'un virus ou d'un programme indésirable.

Pour le composant ProActiv de la protection temps réel, il n'y a aucune option d'action configurable : un résultat positif est toujours signalé dans la fenêtre **Protection temps réel : découverte d'un comportement suspect d'une application**.

Options d'action pour le scanner :

- **Interactif**

  En mode d'action interactif, les résultats positifs de la recherche du scanner sont signalés dans une boîte de dialogue. Ce paramètre est activé par défaut.
  Lors de la **recherche du scanner**, vous recevez à l'issue de la recherche un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers concernés ou quitter le scanner.

- **Automatique**

  En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable.

Options d'action pour la protection temps réel :

- **Interactif**

  En mode d'action interactif, l'accès aux données est refusé et une notification s'affiche sur le Bureau. Dans la notification affichée sur le Bureau, vous avez la possibilité de supprimer le logiciel malveillant trouvé, ou de le transmettre au composant Scanner via le bouton **Détails** pour un traitement du virus. Le scanner

signale le résultat positif dans une fenêtre où un menu contextuel vous propose différentes options pour traiter le fichier concerné (voir Résultat positif > Scanner).

- **Automatique**

  En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable.

Options d'actions pour la protection e-mail et la protection Web :

- **Interactif**

  En mode d'action interactif, une boîte de dialogue s'affiche en cas de détection d'un virus ou d'un programme indésirable, vous permettant de choisir ce qu'il doit advenir de l'objet concerné. Ce paramètre est activé par défaut.

- **Automatique**

  En mode d'action automatique, l'action que vous avez choisie dans cette zone est exécutée automatiquement en cas de détection d'un virus ou d'un programme indésirable.

Mode d'action interactif

- En mode d'action interactif, vous réagissez aux virus et programmes indésirables détectés en sélectionnant dans le message une **Action pour les objets contaminés** et exécutez l'action en cliquant sur **Confirmer**.

Les actions de traitement des objets concernés suivantes sont disponibles :

> **Remarque**
> Les actions disponibles à la sélection dépendent du système d'exploitation, du composant de protection (Scanner Avira, Protection temps réel Avira, Protection e-mail Avira, Protection Web Avira) qui signale le résultat positif, et du logiciel malveillant détecté.

Actions du scanner et de la protection temps réel (sans résultat positif détecté par ProActiv) :

- **Réparer**

  Le fichier est réparé.
  Cette option n'est activable que si une réparation du fichier trouvé est possible.

- **Renommer**

  Le fichier est renommé en **.vir*. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés et renommés ultérieurement.

- **Quarantaine**

Le fichier est compressé dans un format spécial (*.qua*) et déplacé dans le répertoire de quarantaine *INFECTED* sur votre disque dur pour empêcher tout accès direct. Les fichiers de ce répertoire peuvent ensuite être réparés en quarantaine ou - si nécessaire - envoyés à Avira.

- **Supprimer**

  Le fichier est supprimé. Cette procédure est beaucoup plus rapide que le processus d'**écrasement et de suppression**.
  Si le résultat positif est un virus de secteur d'amorçage, le secteur d'amorçage est effacé en cas de suppression. Un nouveau secteur d'amorçage est écrit.

- **Ignorer**

  Aucune action supplémentaire n'est effectuée. Le fichier concerné reste actif sur votre ordinateur.

- **Écraser et supprimer**

  Le fichier est écrasé par un modèle standard puis supprimé. Il ne peut plus être restauré.

> **Avertissement**
> Risque de perte de données et de dommages sur le système d'exploitation. Utilisez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant.

- **Toujours ignorer**

  Option d'action en cas de résultat positif avec la protection temps réel : aucune action supplémentaire n'est effectuée par la protection temps réel. L'accès au fichier est autorisé. Tous les accès ultérieurs à ce fichier sont autorisés et ne sont plus signalés jusqu'au redémarrage de l'ordinateur ou jusqu'à la mise à jour du fichier de définitions des virus.

- **Copier en quarantaine**

  Option d'action en cas de détection d'un rootkit : le programme trouvé est copié en quarantaine.

- **Réparer le secteur d'amorçage | Télécharger l'outil de réparation**

  Options d'action en cas de détection de secteurs d'amorçage infectés : des options d'action pour la réparation de lecteurs de disquettes sont disponibles. Si aucune réparation n'est possible avec votre produit Avira, vous pouvez télécharger un outil spécial pour la détection et la suppression de virus de secteur d'amorçage.

> **Remarque**
> Si vous appliquez des actions sur des processus en cours, les processus concernés sont arrêtés avant l'exécution de l'action.

Action de la protection temps réel en cas de résultat positif avec le composant ProActiv (message d'actions suspectes d'une application) :



- **Programme fiable**

  L'exécution de l'application se poursuit. Le programme est ajouté à la liste des applications autorisées, et il est exclu de la surveillance effectuée par le composant ProActiv. Lors de l'ajout à la liste des applications autorisées, le type de surveillance est définie sur *Contenu*. Cela signifie que l'application n'est exclue d'une surveillance par le composant ProActiv que si le contenu reste inchangé (voir Filtre des applications : applications à exclure).

- **Bloquer le programme une fois**

  L'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le composant ProActiv continue à surveiller les actions de l'application.

- **Toujours bloquer ce programme**

  L'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le programme est ajouté à la liste des applications à bloquer et ne peut plus être exécuté (voir Filtre des applications : applications à bloquer).

- **Ignorer**

  L'exécution de l'application se poursuit. Le composant ProActiv continue à surveiller les actions de l'application.

Actions de la protection e-mail : e-mails entrants

- **Déplacer en quarantaine**

  L'e-mail, y compris toutes les pièces jointes, est déplacé en quarantaine. L'e-mail contaminé est supprimé. Le corps et les pièces jointes éventuelles de l'e-mail sont remplacés par un texte standard.

- **Supprimer l'e-mail**

  L'e-mail contaminé est supprimé. Le corps et les pièces jointes éventuelles sont remplacés par un texte standard.

- **Supprimer la pièce jointe**

  La pièce jointe contaminée est remplacée par un texte standard. Si le corps de l'e-mail est contaminé, celui-ci est supprimé et également remplacé par un texte standard. L'e-mail lui-même est délivré.

- **Déplacer la pièce jointe en quarantaine**

  La pièce jointe concernée est placée en quarantaine puis supprimée (remplacée par un texte standard). Le corps de l'e-mail est délivré. La pièce jointe contaminée peut être délivrée plus tard par le gestionnaire de quarantaines.

- **Ignorer**

  L'e-mail concerné est délivré.

> **Avertissement**
> Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Choisissez l'option **Ignorer** uniquement dans des cas

exceptionnels le justifiant. Désactivez l'aperçu dans Microsoft Outlook, n'ouvrez en aucun cas les pièces jointes par double-clic.

Actions de la protection e-mail : e-mails sortants

- **Déplacer l'e-mail en quarantaine (ne pas envoyer)**

  L'e-mail, y compris toutes les pièces jointes, sont copiés dans la quarantaine et ne sont pas envoyés. L'e-mail reste dans la boîte d'envoi de votre client de messagerie. Vous recevez un message d'erreur dans votre programme de messagerie. La présence de logiciels malveillants est contrôlée dans cet e-mail à chaque processus d'envoi ultérieur de votre compte de messagerie.

- **Bloquer l'envoi d'e-mails (ne pas envoyer)**

  L'e-mail n'est pas envoyé et reste dans la boîte d'envoi de votre client de messagerie. Vous recevez un message d'erreur dans votre programme de messagerie. La présence de logiciels malveillants est contrôlée dans cet e-mail à chaque processus d'envoi ultérieur de votre compte de messagerie.

- **Ignorer**

  L'e-mail concerné est envoyé.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur l'ordinateur du destinataire de l'e-mail.

Actions de la protection Web :

- **Refuser l'accès**

  La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Un message d'erreur de refus d'accès s'affiche dans le navigateur Web.

- **Quarantaine**

  La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine. Le fichier concerné peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center.

- **Ignorer**

  La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par la protection Web.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Choisissez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant.

> **Remarque**
> Nous conseillons de déplacer en quarantaine un fichier suspect qui ne peut être réparé.

> **Remarque**
> Envoyez-nous également les fichiers signalés par l'heuristique pour analyse. Vous pouvez télécharger ces fichiers par ex. via notre site Web : http://www.avira.com/sample-upload
> Vous identifiez les fichiers signalés par l'heuristique à la désignation ?rh-cbt_end ?>*HEUR/* or *HEURISTIC/* , antéposée aux noms des fichiers, par ex : *HEUR/testfile.**.

4.3.11 Quarantaine : traiter les fichiers (*.qua) en quarantaine

Pour traiter les fichiers en quarantaine, procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.
- Vérifiez de quels fichiers il s'agit pour pouvoir recharger les originaux d'un autre emplacement sur votre ordinateur, le cas échéant.

Si vous souhaitez afficher des informations plus détaillées sur un fichier :

- Sélectionnez le fichier et cliquez sur [i].
  - ↳ La boîte de dialogue **Propriétés** s'affiche avec des informations supplémentaires sur le fichier.

Si vous souhaitez à nouveau contrôler un fichier :

La vérification d'un fichier est recommandée quand le fichier de définitions de virus de votre produit Avira a été actualisé et qu'il y a un doute de fausse alerte. De cette façon, vous pouvez confirmer une fausse alerte lors du nouveau contrôle et restaurer le fichier.

- Sélectionnez le fichier et cliquez sur [loupe].
  - ↳ L'absence de virus et logiciels malveillants est contrôlée sur le fichier avec les paramètres de la recherche directe.
  - ↳ Après le contrôle, la boîte de dialogue **Statistiques de contrôle** s'affiche avec les statistiques sur l'état du fichier avant et après le deuxième contrôle.

Si vous souhaitez supprimer un fichier :

- Sélectionnez le fichier et cliquez sur [X].
- Confirmez votre sélection avec **Oui**.



Si vous souhaitez charger le fichier sur un serveur Web de l'Avira Malware Research Center en vue d'une analyse :

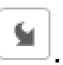
- Sélectionnez le fichier que vous souhaitez télécharger.
- Cliquez sur .
  - ↳ La boîte de dialogue *Chargement du fichier* s'ouvre, avec un formulaire pour la saisie de vos coordonnées.
- Indiquez les données complètes.
- Sélectionnez un type : **Fichier suspect** ou **Doute de fausse alerte**.
- Sélectionnez un format de réponse : **HTML**, **Texte**, **HTML & texte**.
- Cliquez sur **OK.**
  - ↳ Le fichier est chargé sur un serveur Web de l'Avira Malware Research Center.

> **Remarque**
> Dans les cas suivants, une analyse par l'Avira Malware Research Center est recommandée :
> **Résultat heuristique positif (fichier suspect)** : lors d'une recherche, votre produit Avira a classé un fichier comme suspect et l'a placé en quarantaine : dans la boîte de dialogue de détection de virus ou dans le fichier rapport de la recherche, il a été recommandée de faire analyser le fichier par l'Avira Malware Research Center.
> **Fichier suspect** : vous considérez un fichier comme suspect et l'avez de ce fait ajouté à la quarantaine, mais le contrôle du fichier quant à la présence de virus et de logiciels malveillants est négatif.
> **Doute de fausse alerte** : vous supposez que la détection de virus est une fausse alerte : votre produit Avira signale la détection d'un virus dans un fichier, lequel n'est cependant, selon toute vraisemblance, pas infecté par un logiciel malveillant.

> **Remarque**
> La taille des fichiers que vous téléchargez est limitée à 20 Mo au format non compressé ou à 8 Mo en format compressé.

> **Remarque**
> Vous ne pouvez télécharger qu'un seul fichier à la fois.

Si vous souhaitez exporter les propriétés de l'objet en quarantaine dans un fichier texte :

- Sélectionnez l'objet en quarantaine et cliquez sur .

↳ Un fichier texte s'ouvre avec les données relatives à l'objet en quarantaine sélectionné.

▶ Enregistrez le fichier texte.

Vous pouvez également restaurer les fichiers en quarantaine (voir chapitre : Quarantaine : restaurer les fichiers en quarantaine).

4.3.12 Restaurer les fichiers en quarantaine

En fonction du système d'exploitation, diverses icônes sont disponibles pour la restauration :

- Sous Windows XP :
  - Cette icône vous permet de restaurer les fichiers dans le répertoire d'origine.
  - Cette icône vous permet de restaurer des fichiers dans un répertoire de votre choix.
- Sous Windows Vista :

  Sous Microsoft Windows Vista, le Control Center n'a pour le moment que des droits restreints (par exemple, pour l'accès aux répertoires et aux fichiers). Le Control Center ne peut exécuter certaines actions et accéder aux fichiers qu'avec des droits d'administrateur étendus. Ces droits d'administrateur étendus doivent être attribués à chaque démarrage d'une recherche via un profil de recherche.
  - Cette icône vous permet de restaurer des fichiers dans un répertoire de votre choix.
  - Cette icône vous permet de restaurer les fichiers dans le répertoire d'origine. Si des droits d'administrateur sont nécessaires pour accéder à ce répertoire, une demande s'affiche.

Pour restaurer des fichiers en quarantaine, procédez de la manière suivante :

> **Avertissement**
> Risque de perte de données et de dommages sur le système d'exploitation de l'ordinateur. N'utilisez la fonction **Restaurer l'objet sélectionné** que dans des cas exceptionnels. Veillez à ne restaurer que des fichiers qui ont pu être réparés au cours d'une nouvelle recherche.

✓ Fichier recontrôlé et réparé par une recherche.

▶ Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.

> **Remarque**
> Il n'est possible de restaurer les e-mails et pièces jointes d'e-mails qu'avec l'option et avec l'extension **.eml*.

Si vous souhaitez restaurer un fichier à son emplacement d'origine :

- Sélectionnez le fichier et cliquez sur l'icône (Windows XP , Windows Vista).

Cette option n'est pas disponible pour les e-mails.

> **Remarque**
> Il n'est possible de restaurer les e-mails et pièces jointes d'e-mails qu'avec l'option et avec l'extension **.eml*.

↳ Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

↳ Le fichier est restauré dans le répertoire à partir duquel il avait été placé en quarantaine.

Si vous souhaitez restaurer un fichier dans un répertoire particulier :

- Sélectionnez le fichier et cliquez sur .

↳ Le système vous demande si vous souhaitez restaurer le fichier.

- Cliquez sur **Oui**.

↳ La fenêtre Windows par défaut, permettant de sélectionner un répertoire, s'affiche (*Enregistrer sous*).

- Sélectionnez le répertoire dans lequel le fichier doit être restauré et validez.

↳ Le fichier est restauré dans le répertoire choisi.

4.3.13 Quarantaine : déplacer un fichier suspect en quarantaine

Vous pouvez déplacer manuellement un fichier suspect en quarantaine de la manière suivante :

- Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* **> Quarantaine**.
- Cliquez sur .

↳ La fenêtre standard Windows pour sélectionner un fichier s'affiche.

- Choisissez un fichier et validez avec **Ouvrir**.

↳ Le fichier est déplacé en quarantaine.

Vous pouvez vérifier les fichiers en quarantaine avec le scanner Avira (voir chapitre : Quarantaine : traiter les fichiers (*.qua) en quarantaine).

4.3.14 Profil de recherche : compléter ou supprimer un type de fichier dans un profil de recherche

Voici comment établir pour un profil de recherche qui scanne des types de fichiers supplémentaires ou exclut certains types de fichiers lors de la recherche (possible uniquement en cas de sélection manuelle et de profils de recherche définis par l'utilisateur) :

✓ Dans le Control Center, accédez à la rubrique *SÉCURITÉ PC* **> Scanner**.

- Cliquez avec le bouton droit de la souris sur le profil de recherche que vous souhaitez éditer.

  ↳ Un menu contextuel s'affiche.

- Sélectionnez l'entrée **Filtre de fichiers**.
- Déployez le menu contextuel en cliquant sur le petit triangle à droite du menu contextuel.

  ↳ Les entrées **Standard**, **Contrôler tous les fichiers** et **Personnalisé** apparaissent.

- Sélectionnez l'entrée **Personnalisé**.

  ↳ La boîte de dialogue **Extensions de fichiers** s'affiche avec une liste de tous les types de fichiers qui sont parcourus avec le profil de recherche.

Si vous voulez exclure un type de fichier de la recherche :

- Sélectionnez le type de fichier et cliquez sur **Supprimer**.

Si vous voulez ajouter un type de fichier à la recherche :

- Sélectionnez le type de fichier.
- Cliquez sur **Ajouter** et saisissez l'extension de fichier du type de fichier dans le champ de saisie.

  Utilisez au maximum 10 caractères et ne tapez pas le point initial. Les caractères de remplacement (* et ?) sont autorisés.

4.3.15 Profil de recherche : créer un raccourci sur le Bureau pour le profil de recherche

Le raccourci sur le Bureau vers un profil de recherche vous permet de démarrer une recherche directe depuis votre Bureau, sans accéder au Control Center de votre produit Avira.

Pour créer un raccourci vers le profil de recherche sur le Bureau, procédez de la manière suivante :

✓ Dans le Control Center, accédez à la rubrique *SÉCURITÉ PC* **> Scanner**.

▶ Sélectionnez le profil de recherche vers lequel vous souhaitez créer un raccourci.

▶ Cliquez sur l'icône .

↳ Le raccourci sur le Bureau est créé.

4.3.16 Événements : filtrer les événements

Dans le Control Center, sous *ADMINISTRATION* **> Événements** sont affichés tous les événements générés par les composants programme de votre produit Avira (comme avec l'affichage des événements de votre système d'exploitation Windows). Les composants programme sont, par ordre alphabétique, les suivants :

- Protection Web
- Protection temps réel
- Protection e-mail
- Service d'assistance
- Planificateur
- Scanner
- Updater
- ProActiv

Les types d'événements suivants s'affichent :

- *Information*
- *Avertissement*
- *Erreur*
- *Résultat positif*

Voici comment filtrer les événements affichés :

▶ Dans le Control Center, sélectionnez la rubrique *ADMINISTRATION* > Événements .

▶ Activez les cases à cocher des composants programme pour afficher les événements des composants activés.

- OU -

Décochez les cases à cocher des composants programme pour masquer les événements des composants désactivés.

▶ Activez la case à cocher des types d'événements pour afficher ces événements.

- OU -

Décochez les cases des types d'événements pour masquer ces événements.

4.3.17 Protection e-mail : exclure des adresses e-mail du contrôle

Pour exclure des adresses e-mail (expéditeur) du contrôle par la protection e-mail (mise sur liste blanche), procédez de la façon suivante :

- Dans le Control Center, sélectionnez la rubrique *SÉCURITÉ INTERNET* **> Protection e-mail**.
  - ↳ Vous voyez dans la liste les e-mails reçus.
- Sélectionnez l'e-mail que vous souhaitez exclure du contrôle de la protection e-mail.
- Cliquez sur l'icône souhaitée pour exclure l'e-mail du contrôle par la protection e-mail :

L'adresse e-mail sélectionnée ne sera plus contrôlée à l'avenir pour rechercher virus et programmes indésirables.

- ↳ L'adresse e-mail de l'expéditeur est ajoutée à la liste d'exceptions et n'est plus contrôlée quant à l'absence de virus et de logiciels malveillants.

Avertissement
N'excluez du contrôle par la protection e-mail que les adresses e-mail absolument dignes de confiance.

Remarque
Dans la configuration, sous Protection e-mail > Généralités > Exceptions, vous pouvez intégrer des adresses e-mail supplémentaires dans la liste d'exceptions ou en supprimer.

5. Résultat positif

5.1 Aperçu

En cas de résultats positifs, votre produit Avira peut exécuter automatiquement certaines actions ou réagir de manière interactive. En mode interactif, si un virus est détecté, une fenêtre de dialogue s'ouvre pour vous permettre de déclencher une autre opération sur le virus (Supprimer, Ignorer etc.). En mode automatique, une option permet d'afficher un message d'avertissement en cas de résultat positif. Le message indique l'action qui a été exécutée automatiquement.

Ce chapitre vous fournit toutes les informations sur les messages d'un résultat positif, triées par module.

- voir chapitre Scanner : mode d'action interactif
- voir chapitre Scanner : envoyer les fichiers à la protection Cloud
- voir chapitre Protection temps réel
- voir chapitre Protection temps réel : comportement suspect
- voir chapitre Protection e-mail : e-mails entrants
- voir chapitre Protection e-mail : e-mails sortants
- voir chapitre Protection Web

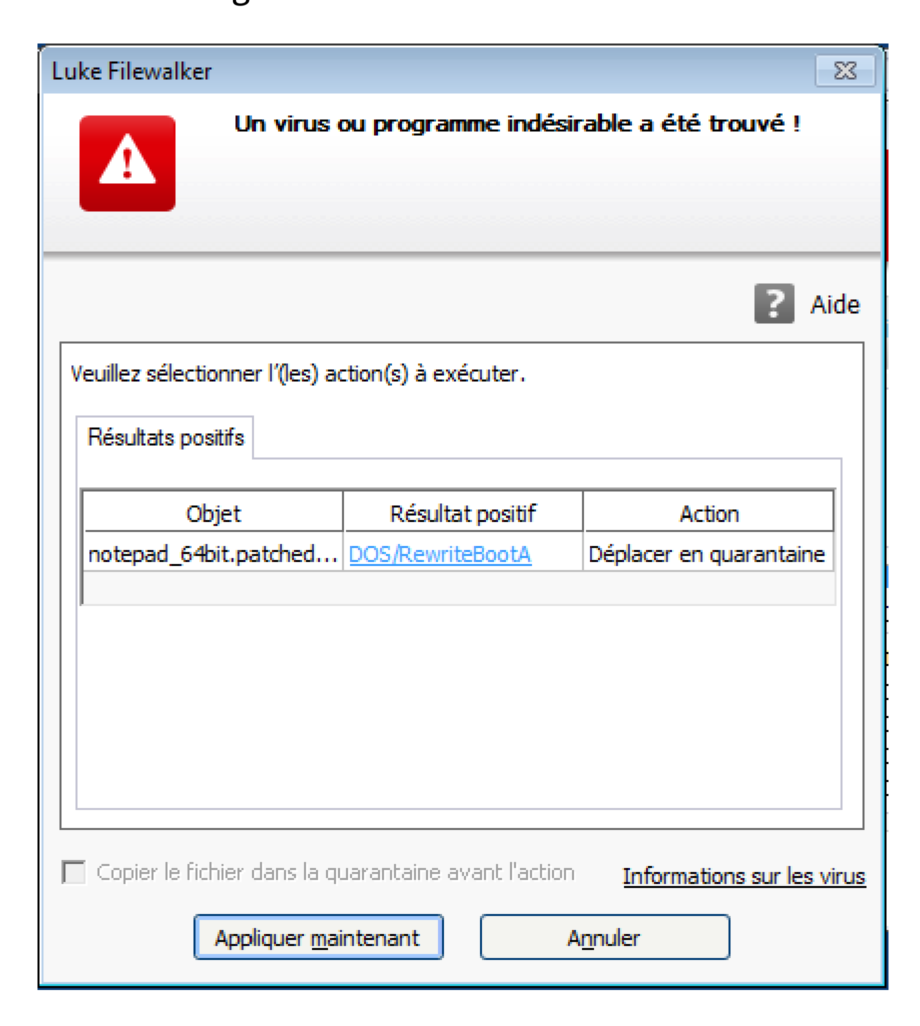
5.2 Mode d'action interactif

Une fois que le scanner a terminé d'analyser les fichiers, vous recevez un message d'avertissement contenant la liste des fichiers concernés, si vous avez choisi comme mode d'action pour les virus détectés le mode *interactif* (voir la rubrique de configuration Scanner > Recherche > Action si résultat positif).
Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers concernés ou quitter le scanner.

> **Remarque**
> Si la fonction de consignation est activée, le scanner enregistre chaque résultat positif dans le fichier rapport.



5.2.1 Message d'avertissement



5.2.2 Résultat positif, erreurs, avertissements

Les onglets **Résultat positif**, **Erreurs** et **Avertissements** affichent des informations détaillées et des options d'action relatives aux virus détectés ainsi que des avertissements :

- **Résultat positif :**
  - *Objet :* nom du fichier concerné
  - *Résultat positif :* nom du virus ou programme indésirable trouvé
  - *Action :* action sélectionnée pour le traitement du fichier concerné
    Dans le menu contextuel de l'action affichée, vous pouvez sélectionner d'autres actions pour le traitement du logiciel malveillant.
- **Erreurs :** messages concernant les erreurs survenues pendant la recherche
- **Avertissements :** messages d'avertissement se rapportant aux virus détectés

> **Remarque**
> Les informations suivantes s'affichent dans l'info-bulle de l'objet : nom du fichier



concerné et chemin complet, nom du virus, action exécutée au moyen du bouton **Appliquer maintenant**.

Remarque
L'action par défaut du scanner est proposée comme action standard à exécuter. L'action par défaut du scanner concernant le traitement des fichiers infectés consiste à déplacer le fichier contaminé en quarantaine.

5.2.3 Actions du menu contextuel

Remarque
Si le résultat positif concerne une concordance heuristique (HEUR/), un logiciel de compression des fichiers exécutables inhabituel (PCK/) ou un fichier à extension déguisée (HEUR-DBLEXT/), le mode interactif ne propose que les options Déplacer en quarantaine et Ignorer. En mode automatique, le résultat positif est déplacé automatiquement en quarantaine.
Cette restriction évite que les fichiers trouvés pour lesquels il peut s'agir d'une fausse alerte soient effacés (supprimés) directement de votre ordinateur. Le fichier peut être restauré à tout moment à l'aide du gestionnaire de quarantaines.

Réparer

Si cette option est activée, le scanner répare le fichier concerné.

Remarque
L'option **Réparer** est activable uniquement si la réparation du fichier trouvé est possible.

Quarantaine

Si cette option est activée, le scanner déplace le fichier en quarantaine. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center. Selon le fichier, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus d'écrasement et de suppression.



Écraser et supprimer

Si l'option est activée, le scanner remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Renommer

Si l'option est activée, le scanner renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Le fichier peut être réparé ultérieurement et à nouveau renommé.

Ignorer

Si cette option est activée, le fichier est conservé.

Toujours ignorer

Option d'action en cas de résultat positif avec la protection temps réel : aucune action supplémentaire n'est effectuée par la protection temps réel. L'accès au fichier est autorisé. Tous les accès ultérieurs à ce fichier sont autorisés et ne sont plus signalés jusqu'au redémarrage de l'ordinateur ou jusqu'à la mise à jour du fichier de définitions des virus.

Avertissement
Si vous sélectionnez les options **Ignorer** ou **Toujours ignorer**, les fichiers concernés restent actifs sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

5.2.4 Particularités en cas de détection de secteurs d'amorçage infectés, de rootkits et de logiciels malveillants actifs

En cas de détection de secteurs d'amorçage infectés, des options d'action pour la réparation des secteurs d'amorçage sont disponibles :

Réparer le secteur d'amorçage de 722 Ko | 1,44 Mo | 2,88 Mo | 360 Ko | 1,2 Mo

Ces options sont disponibles pour les lecteurs de disquettes.

Télécharger le CD de secours

Cette option vous permet d'accéder au site Web d'Avira, où vous pouvez télécharger un outil spécial pour la détection et la suppression de virus de secteur d'amorçage.

Si vous appliquez des actions sur des processus en cours, les processus concernés sont arrêtés avant l'exécution de l'action.

5.2.5 Boutons et liens

Bouton / Lien	Description
Appliquer maintenant	Les actions sélectionnées sont exécutées pour traiter tous les fichiers concernés.
Annuler	Le scanner est arrêté sans autre opération. Les fichiers concernés sont conservés sur votre ordinateur.
Aide	Ce bouton ou lien vous permet d'ouvrir cette page de l'aide en ligne.

> **Avertissement**
> N'exécutez l'action **Annuler** que dans des cas exceptionnels le justifiant. Les fichiers concernés restent actifs sur votre ordinateur en cas d'interruption. D'importants dégâts peuvent être causés sur votre ordinateur.

5.2.6 Particularités en cas de résultats positifs lorsque la protection Web est désactivée

Si vous avez désactivé le protection Web, la protection temps réel signale la détection de logiciels malveillants actifs par un message au cours de l'analyse du système. Vous pouvez créer un point de restauration système avant la réparation.

✓ La fonction de restauration système doit être activée dans votre système d'exploitation Windows.

- Cliquez sur l'option **Afficher les détails** dans le message.
  - ↳ La fenêtre *Système en cours d'analyse* s'affiche.
- Activez l'option **Créer un point de restauration système avant la réparation**.
- Cliquez sur **Appliquer**.
  - ↳ Un point de restauration système est créé. Vous pouvez donc effectuer une restauration système le cas échéant.

5.3 Envoyer les fichiers à la protection Cloud

Une liste d'emplacements de fichiers est créée lors de chaque **contrôle rapide du système**, ciblant les logiciels malveillants. Dans cette liste figurent par exemple les processus, les programmes de démarrage et les programmes de services en cours. Les fichiers de programmes inconnus sont chargés dans le système d' Avira Protection Cloud en vue de leur analyse.

Si, lors de l'installation personnalisée ou de la configuration de la **protection étendue**, vous avez activé l'option **Confirmer manuellement si des fichiers suspects doivent être envoyés à Avira**, vous pouvez consulter la liste des fichiers suspects et déterminer vous-même quels sont les fichiers que vous souhaitez télécharger sur l'Avira Protection Cloud. Par défaut, tous les fichiers suspects sont sélectionnés pour téléchargement.

Remarque
Si vous avez activé la fonction de consignation **avancée** lors de la configuration du scanner, le fichier rapport mentionne le suffixe *(Cloud)* pour vous permettre d'identifier les avertissements de l'Avira Protection Cloud.

5.3.1 Informations affichées

Liste des fichiers suspects qui doivent être téléchargés sur l'Avira Protection Cloud.

- *Envoyer ? :* vous pouvez sélectionner les fichiers que vous souhaitez télécharger sur l'Avira protection Cloud.
- *Fichier :* nom du fichier suspect.
- *Chemin :* chemin du fichier suspect.

Toujours envoyer les fichiers automatiquement

Tant que cette option reste active, les fichiers suspects sont automatiquement envoyés, sans confirmation manuelle, à l'Avira Protection Cloud pour être analysés après chaque **contrôle rapide du système**.

5.3.2 Boutons et liens

Bouton / Lien	Description
Envoyer	Les fichiers sélectionnés sont envoyés à l'Avira Protection Cloud.
Annuler	Le scanner est arrêté sans autre opération. Les fichiers concernés sont conservés sur votre système.
Aide	Cette page de l'aide en ligne est ouverte.
Présentation de la Protection Cloud	La page Web présentant des informations sur l'Avira Protection Cloud s'affiche.

Thèmes apparentés :

- Configuration de la protection étendue

- Installation personnalisée
- Configuration des rapports
- Affichage des rapports

5.4 Protection temps réel

Si un virus est détecté par la protection temps réel, l'accès au fichier est refusé et une notification s'affiche sur le Bureau, si vous avez choisi comme mode d'action pour les virus détectés le mode *interactif* (voir la rubrique de configuration Protection temps réel > Recherche > Action si résultat positif).

Notification

La notification affiche les informations suivantes :

- Date et heure du résultat positif
- Chemin et nom du fichier concerné
- Nom du logiciel malveillant

> **Remarque**
> La sélection du mode de démarrage standard pour la protection temps réel (démarrage normal) et une connexion rapide du compte utilisateur a notamment pour conséquence, lors du démarrage de l'ordinateur, que les programmes lancés automatiquement au démarrage du système ne sont pas analysés, car ceux-ci sont démarrés avant la fin du chargement complet de la protection temps réel.

En mode interactif, vous disposez des options suivantes :

Supprimer

Le fichier concerné est transmis au composant **Scanner** qui le supprime. Aucun autre message ne s'affiche plus.

Détails

Le fichier concerné est transmis au composant **Scanner**. Le scanner signale le résultat positif dans une fenêtre où vous avez différentes options pour traiter le fichier concerné.

> **Remarque**
> Veuillez tenir compte des remarques relatives au traitement des virus sous Résultat positif > Scanner.



> **Remarque**
> L'action *Quarantaine* est prédéfinie par défaut dans le message du scanner. Vous pouvez sélectionner d'autres actions via un menu contextuel.

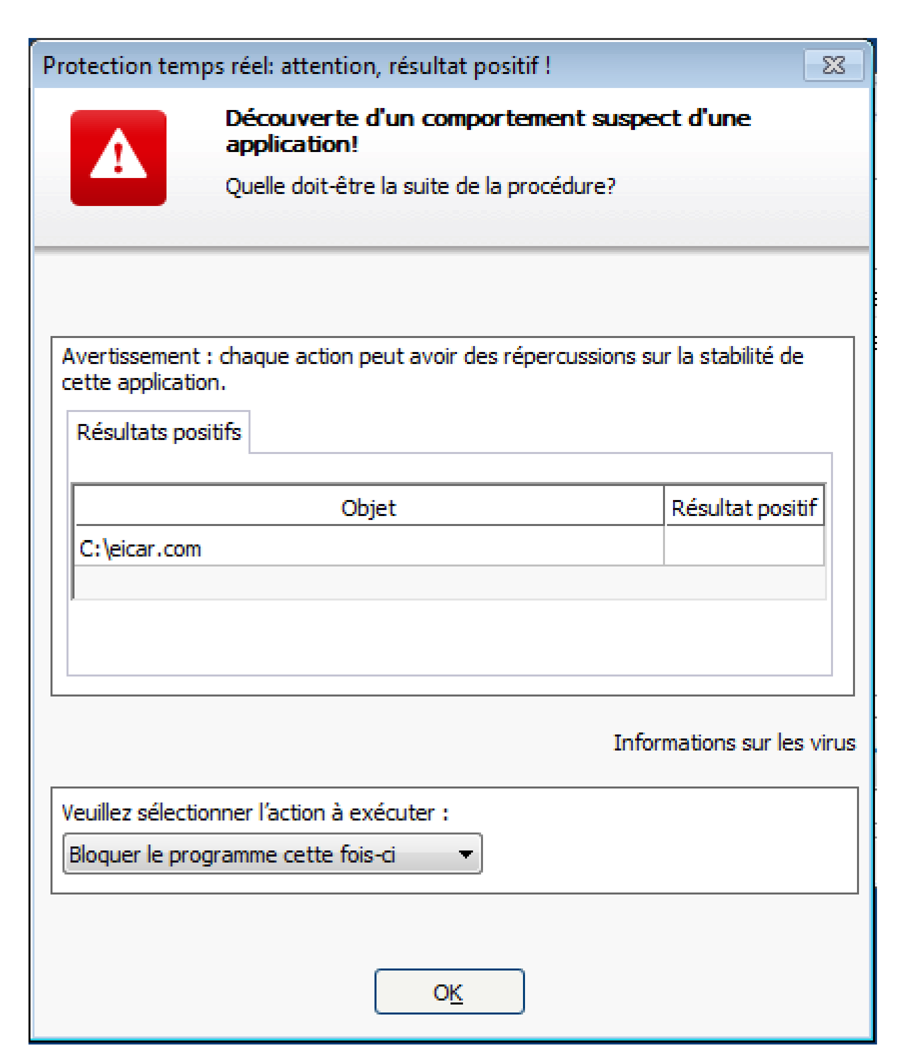
Fermer

Le message se ferme. Le traitement de virus est interrompu.

5.5 Comportement suspect

Quand vous activez le composant ProActiv de la protection temps réel, celui-ci surveille les actions des applications et contrôle l'absence de comportement suspect typique d'un logiciel malveillant. En cas de comportement suspect, vous recevez un message d'avertissement. Vous avez plusieurs options pour réagir au résultat positif.

5.5.1 Message d'avertissement de la protection temps réel : découverte d'un comportement suspect d'une application



5.5.2 Nom et chemin du programme suspect détecté actuel

Dans la fenêtre centrale du message s'affichent le nom et le chemin de l'application qui exécute les actions suspectes.

5.5.3 Possibilités de sélection

Programme fiable

Si cette option est activée, l'exécution de l'application se poursuit. Le programme est ajouté à la liste des applications autorisées, et il est exclu de la surveillance effectuée par le composant ProActiv. Lors de l'ajout à la liste des applications autorisées, le type de surveillance est définie sur *Contenu*. Cela signifie que l'application n'est exclue d'une surveillance par le composant ProActiv que si le contenu reste inchangé (voir Filtre des applications : applications autorisées).

Bloquer le programme une fois

Lorsque cette option est activée, l'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le composant ProActiv continue à surveiller les actions de l'application.

Toujours bloquer ce programme

Lorsque cette option est activée, l'application est bloquée, c'est-à-dire que l'exécution de l'application est arrêtée. Le programme est ajouté à la liste des applications à bloquer et ne peut plus être exécuté (voir Filtre des applications : applications à bloquer).

Ignorer

Si cette option est activée, l'exécution de l'application se poursuit. Le composant ProActiv continue à surveiller les actions de l'application.

5.5.4 Boutons et liens

Bouton / Lien	Description
Informations sur les virus	En cliquant sur ce lien - quand la connexion Internet est active - vous arrivez sur une page Internet contenant des informations détaillées sur le virus ou le programme indésirable.
Aide	Ce bouton ou lien vous permet d'ouvrir cette page de l'aide en ligne.

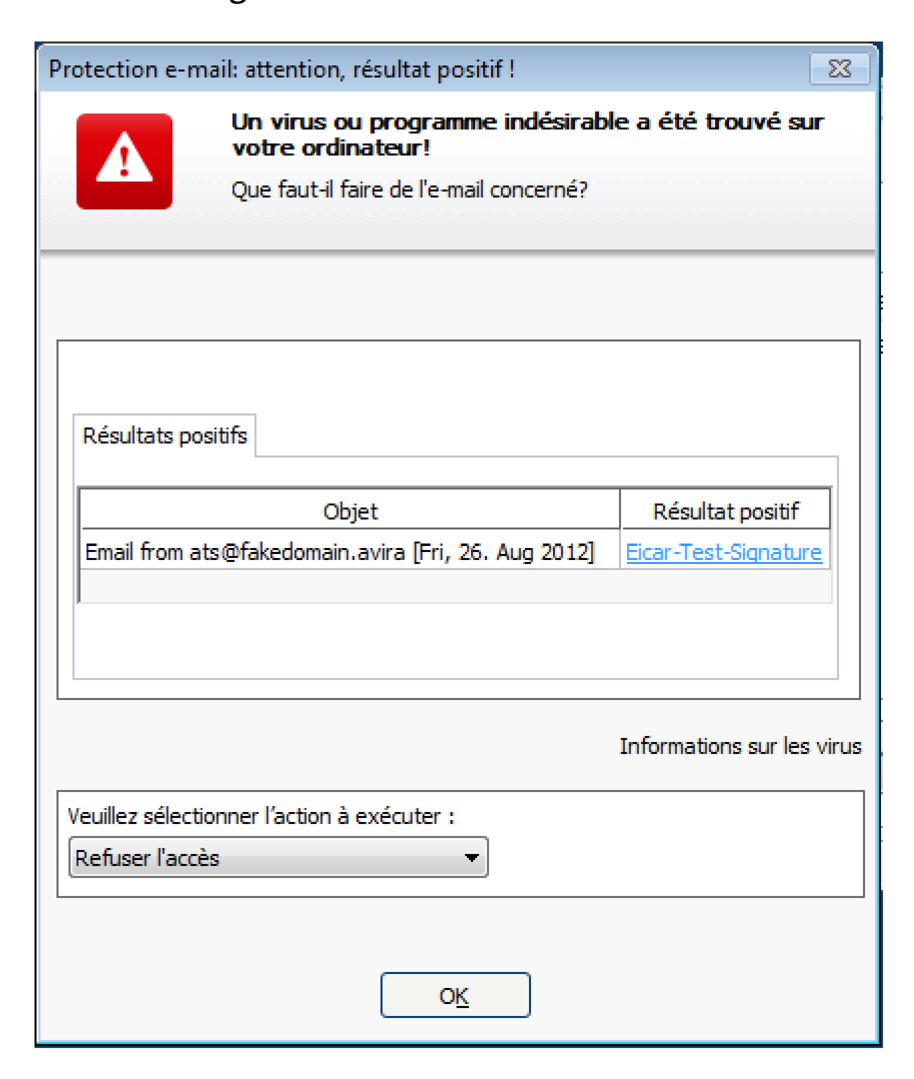


5.6 E-mails entrants

Si un virus est détecté par la protection e-mail, vous recevez un message d'avertissement si vous avez choisi comme mode d'action pour les virus détectés le mode *interactif* (voir la rubrique de configuration Protection e-mail > Recherche > Action si résultat positif). En mode interactif, vous pouvez déterminer dans une fenêtre de dialogue ce qui doit advenir de l'e-mail ou de la pièce jointe.

Vous recevez le message d'avertissement ci-dessous en cas de détection d'un virus dans un e-mail entrant.

5.6.1 Message d'avertissement



5.6.2 Résultats positifs, erreurs, avertissements

Les onglets **Résultats positifs**, **Erreurs** et **Avertissements** affichent des messages et des informations détaillées relatives aux e-mails concernés :

- **Résultats positifs :** objet : e-mail concerné avec indication de l'expéditeur et du moment auquel l'e-mail a été envoyé

Résultat positif : nom du virus ou programme indésirable trouvé

- **Erreurs :** messages concernant les erreurs survenues pendant le contrôle par la protection e-mail
- **Avertissements :** messages d'avertissement se rapportant aux objets concernés

5.6.3 Possibilités de sélection

> **Remarque**
> Si le résultat positif concerne une concordance heuristique (HEUR/), un logiciel de compression des fichiers exécutables inhabituel (PCK/) ou un fichier à extension déguisée (HEUR-DBLEXT/), le mode interactif ne propose que les options Déplacer en quarantaine et Ignorer. En mode automatique, le résultat positif est déplacé automatiquement en quarantaine.
> Cette restriction évite que les fichiers trouvés pour lesquels il peut s'agir d'une fausse alerte soient effacés (supprimés) directement de votre ordinateur. Le fichier peut être restauré à tout moment à l'aide du gestionnaire de quarantaines.

Déplacer en quarantaine

Si cette option est activée, l'e-mail et toutes les pièces jointes sont déplacés en quarantaine. Il peut être délivré ultérieurement par le gestionnaire de quarantaines. L'e-mail contaminé est supprimé. Le corps et les pièces jointes éventuelles de l'e-mail sont remplacés par un texte standard.

Supprimer l'e-mail

Si l'option est activée, l'e-mail contaminé est supprimé si un virus ou un programme indésirable a été détecté. Le corps et les pièces jointes éventuelles sont remplacés par un texte standard.

Supprimer la pièce jointe

Si cette option est activée, la pièce jointe concernée est remplacée par un texte standard. Si le corps de l'e-mail est concerné, il est supprimé et également remplacé par un texte standard. L'e-mail lui-même est délivré.

Déplacer la pièce jointe en quarantaine

Si cette option est activée, la pièce jointe contaminée est placée en quarantaine puis supprimée (remplacée par un texte standard). Le corps de l'e-mail est délivré. La pièce jointe contaminée peut être délivrée plus tard par le gestionnaire de quarantaines.

Ignorer

Si cette option est activée, un e-mail concerné est délivré même si un virus ou un programme indésirable a été détecté.



Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Choisissez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant. Désactivez l'aperçu dans Microsoft Outlook, n'ouvrez en aucun cas les pièces jointes par double-clic.

5.6.4 Boutons et liens

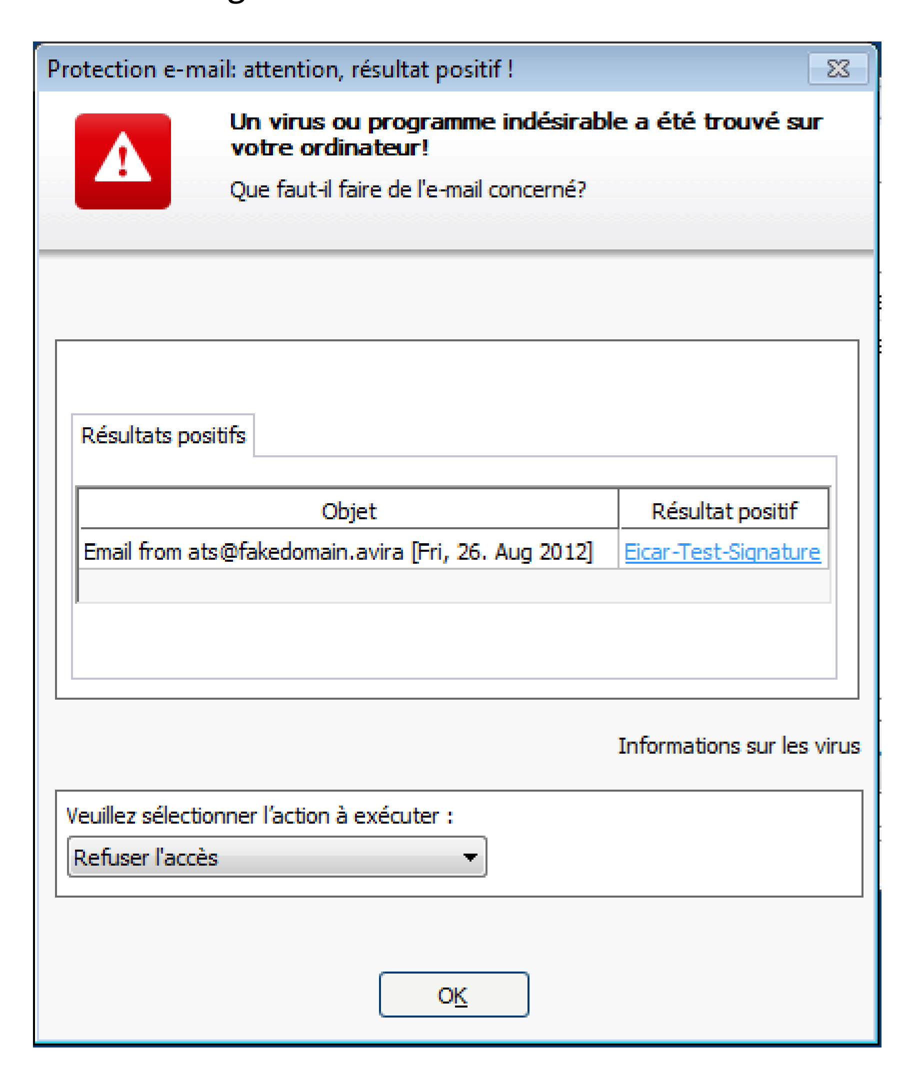
Bouton / Lien	Description
Informations sur les virus	En cliquant sur ce lien - quand la connexion Internet est active - vous arrivez sur une page Internet contenant des informations détaillées sur le virus ou le programme indésirable.
Aide	Ce bouton ou lien vous permet d'ouvrir cette page de l'aide en ligne.

5.7 E-mails sortants

Si un virus est détecté par la protection e-mail, vous recevez un message d'avertissement si vous avez choisi comme mode d'action pour les virus détectés le mode *interactif* (voir la rubrique de configuration Protection e-mail > Recherche > Action si résultat positif). En mode interactif, vous pouvez déterminer dans une fenêtre de dialogue ce qui doit advenir de l'e-mail ou de la pièce jointe.



5.7.1 Message d'avertissement



5.7.2 Résultats positifs, erreurs, avertissements

Les onglets **Résultats positifs**, **Erreurs** et **Avertissements** affichent des messages et des informations détaillées relatives aux e-mails concernés :

- **Résultats positifs :** objet : e-mail concerné avec indication de l'expéditeur et du moment auquel l'e-mail a été envoyé

  Résultat positif : nom du virus ou programme indésirable trouvé
- **Erreurs :** messages concernant les erreurs survenues pendant le contrôle par la protection e-mail
- **Avertissements :** messages d'avertissement se rapportant aux objets concernés



5.7.3 Possibilités de sélection

Déplacer l'e-mail en quarantaine (ne pas envoyer)

Si cette option est activée, l'e-mail et ses pièces jointes sont placés en quarantaine et ne sont pas envoyés. L'e-mail reste dans la boîte d'envoi de votre client de messagerie. Vous recevez un message d'erreur dans votre programme de messagerie. La présence de logiciels malveillants est contrôlée dans cet e-mail à chaque processus d'envoi ultérieur de votre compte de messagerie.

Bloquer l'envoi d'e-mails (ne pas envoyer)

L'e-mail n'est pas envoyé et reste dans la boîte d'envoi de votre client de messagerie. Vous recevez un message d'erreur dans votre programme de messagerie. La présence de logiciels malveillants est contrôlée dans cet e-mail à chaque processus d'envoi ultérieur de votre compte de messagerie.

Ignorer

Si cette option est activée, l'e-mail concerné est envoyé même si un virus ou programme indésirable a été détecté.

Avertissement
Ce faisant, il est possible que des virus et programmes indésirables arrivent sur l'ordinateur du destinataire de l'e-mail.

5.7.4 Boutons et liens

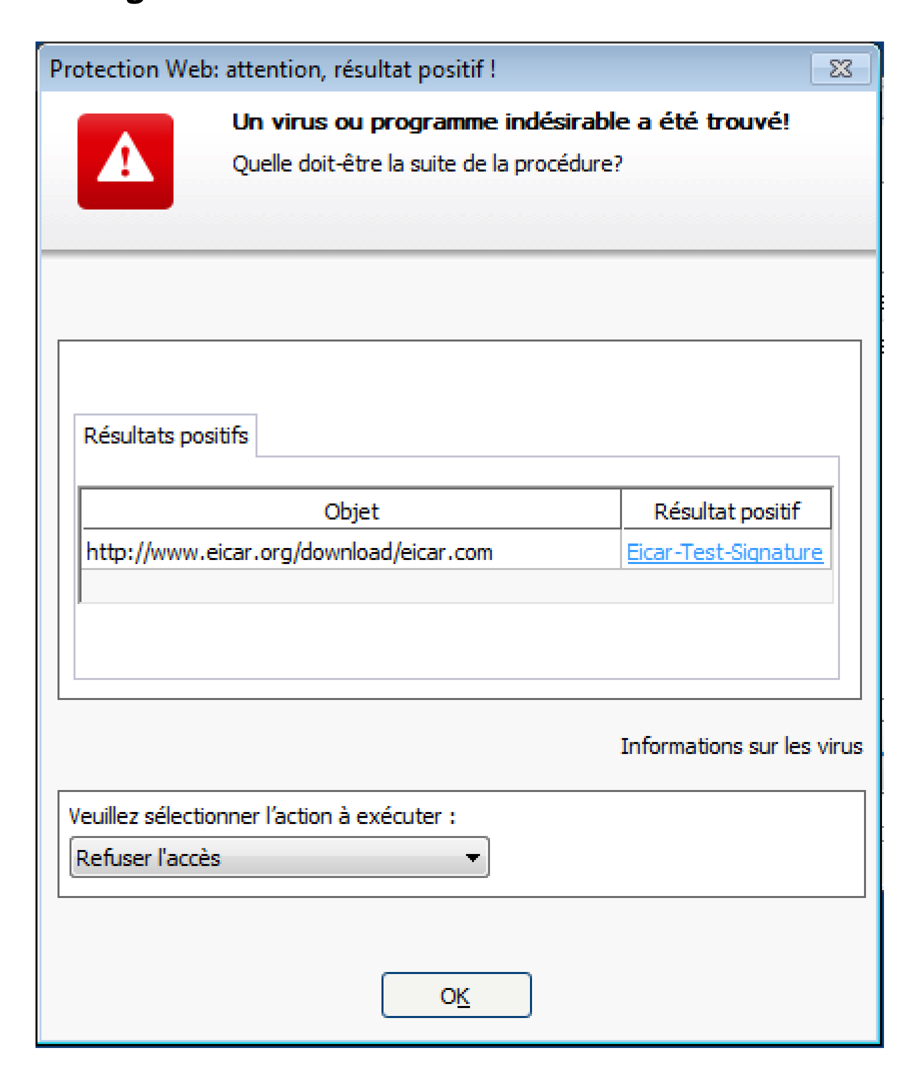
Bouton / Lien	Description
Informations sur les virus	En cliquant sur ce lien - quand la connexion Internet est active - vous arrivez sur une page Internet contenant des informations détaillées sur le virus ou le programme indésirable.
? Aide	Ce bouton ou lien vous permet d'ouvrir cette page de l'aide en ligne.

5.8 Protection Web

Si un virus est détecté par la protection Web, vous recevez un message d'avertissement si vous avez choisi comme mode d'action pour les virus détectés le mode *interactif* (voir la

rubrique de configuration Protection Web > Recherche > Action si résultat positif). En mode interactif, vous pouvez déterminer dans une fenêtre de dialogue ce qui doit advenir des données transférées depuis le serveur Web.

Message d'avertissement



Résultat positif, erreurs, avertissements

Les onglets **Résultat positif**, **Erreurs** et **Avertissements** affichent des messages et des informations détaillées relatives aux virus détectés :

- **Résultat positif :** URL et nom du virus ou programme indésirable trouvé
- **Erreurs :** messages concernant les erreurs survenues pendant le contrôle par la protection Web
- **Avertissements :** messages d'avertissement se rapportant aux virus détectés

Actions possibles

> **Remarque**
> Si le résultat positif concerne une concordance heuristique (HEUR/), un logiciel de compression des fichiers exécutables inhabituel (PCK/) ou un fichier à extension déguisée (HEUR-DBLEXT/), le mode interactif ne propose que les options Déplacer en quarantaine et Ignorer.
> Cette restriction évite que les fichiers trouvés pour lesquels il peut s'agir d'une fausse alerte soient effacés (supprimés) directement de votre ordinateur. Le fichier peut être restauré à tout moment à l'aide du gestionnaire de quarantaines.

Refuser l'accès

La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Un message d'erreur de refus d'accès s'affiche dans le navigateur Web. La protection Web inscrit le résultat positif dans le fichier rapport, dès lors que la fonction de rapport est activée.

Isoler (déplacer en quarantaine)

La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine en cas de détection d'un virus ou d'un logiciel malveillant. Le fichier concerné peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center.

Ignorer

La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par la protection Web.

> **Avertissement**
> Ce faisant, il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. Choisissez l'option **Ignorer** uniquement dans des cas exceptionnels le justifiant.

Boutons et liens

Bouton / Lien	Description
Informations sur les virus	En cliquant sur ce lien - quand la connexion Internet est active - vous arrivez sur une page Internet contenant des informations détaillées sur le virus ou le programme indésirable.
Aide	Ce bouton ou lien vous permet d'ouvrir cette page de l'aide en ligne.



6. Scanner

6.1 Scanner

Grâce au composant Scanner, vous pouvez rechercher de manière ciblée les virus et programmes indésirables (recherche directe). Vous avez les possibilités suivantes pour rechercher des fichiers contaminés :

- **Recherche directe via le menu contextuel**
  La recherche directe via le menu contextuel (bouton droit de la souris - entrée **Contrôler les fichiers sélectionnés avec Avira**) est recommandée si vous voulez contrôler des fichiers et répertoires séparément dans l'explorateur Windows par exemple. Un autre avantage est qu'il n'est pas nécessaire de démarrer le Control Center pour la recherche directe via le menu contextuel.
- **Recherche directe par glisser-déplacer**
  En glissant un fichier ou un répertoire dans la fenêtre de programme du Control Center, le scanner contrôle le fichier ou le répertoire, ainsi que tous les sous-répertoires inclus. Cette procédure est recommandée si vous souhaitez contrôler des fichiers et répertoires séparément, que vous avez par ex. déposés sur votre Bureau.
- **Recherche directe via les profils**
  Cette procédure est recommandée si vous souhaitez contrôler régulièrement certains répertoires et lecteurs (par ex. votre répertoire de travail ou les lecteurs sur lesquels vous déposez régulièrement des fichiers). Il n'est alors plus nécessaire de sélectionner ces répertoires et lecteurs à chaque contrôle, il suffit d'une simple sélection avec le profil correspondant.
- **Recherche directe via le planificateur**
  Le planificateur permet d'effectuer des tâches de contrôle programmées.

Des procédures particulières sont nécessaires lors de la recherche de rootkits, de virus de secteurs d'amorçage et du contrôle de processus actifs. Vous disposez des options suivantes :

- Recherche de rootkits via le profil de recherche **Recherche des rootkits et des logiciels malveillants actifs**
- Contrôle des processus actifs via le profil de recherche **Processus actifs**
- Recherche de virus de secteurs d'amorçage via la commande **Contrôler les virus de secteurs d'amorçage** dans le menu **Extras**

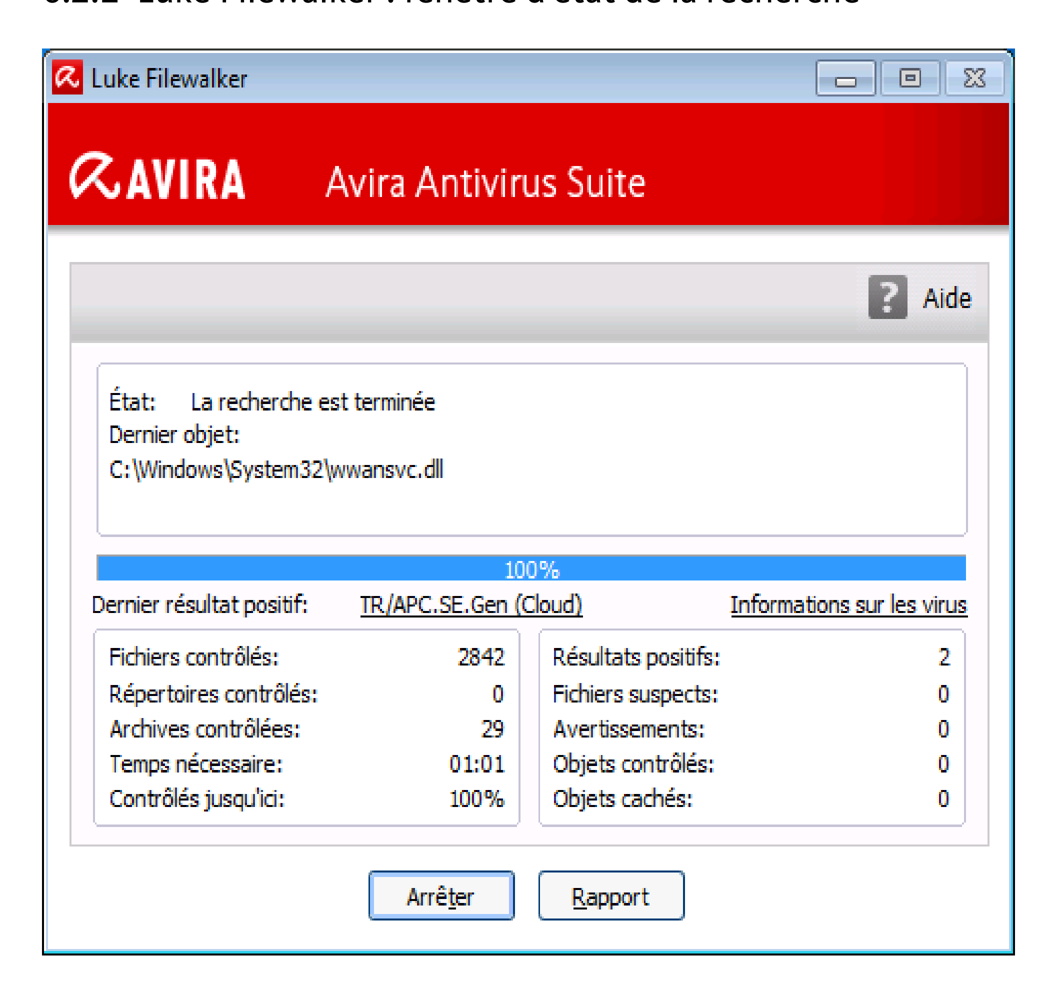
6.2 Luke Filewalker

Pendant la recherche directe, la fenêtre d'état **Luke Filewalker** s'affiche et vous informe sur l'état du contrôle.

Si, dans la configuration du scanner, l'option **Interactif** est sélectionnée dans le groupe **Action si résultat positif**, le système vous demande quoi faire en cas de détection d'un virus ou d'un programme indésirable. Si l'option **Automatique** est sélectionnée, les éventuels résultats positifs sont visibles dans le rapport du scanner.

Une fois la recherche terminée, le système affiche les résultats de la recherche (statistique) ainsi que les messages d'erreur et d'avertissement.

6.2.1 Luke Filewalker : fenêtre d'état de la recherche



Informations affichées

État : il existe différents messages d'état :

- *Initialisation du programme*
- *Recherche d'objets cachés en cours !*
- *Contrôle en cours des processus lancés*
- *Fichier en cours de contrôle*
- *Archive en cours d'initialisation*
- *Libérer de la mémoire*
- *Décompression du fichier*

- *Contrôle en cours des secteurs d'amorçage*
- *Contrôle en cours des secteurs d'amorçage maître*
- *Contrôle en cours du Registre*
- *Le programme va être arrêté !*
- *La recherche a été arrêtée*

Dernier objet : nom et chemin du fichier en cours de contrôle ou qui a été contrôlé en dernier

Dernier résultat positif : il existe différents messages sur le dernier résultat positif :

- *Aucun virus trouvé !*
- Nom du dernier virus ou programme indésirable trouvé

Fichiers contrôlés : nombre de fichiers contrôlés

Répertoires contrôlés : nombre de répertoires contrôlés

Archives contrôlées : nombre d'archives contrôlées

Temps nécessaire : durée de la recherche directe

Contrôlés jusqu'ici : pourcentage de la recherche déjà effectuée

Résultats positifs : nombre de virus et programmes indésirables trouvés

Fichiers suspects : nombre de fichiers signalés par l'heuristique

Avertissements : nombre de messages d'avertissement relatifs à des virus détectés

Objets contrôlés : nombre d'objets contrôlés lors de la recherche de rootkits

Objets cachés : nombre total d'objets cachés qui ont été identifiés

Remarque
Les rootkits ont la propriété de dissimuler des processus et objets comme les entrées de registres ou les fichiers, toutefois chaque objet dissimulé ne prouve pas nécessairement l'existence d'un rootkit. En cas d'objets cachés, il peut également s'agir d'objets inoffensifs. Lors de la recherche, si des objets cachés sont trouvés et s'il n'y a aucun message d'avertissement relatif à des virus détectés, vous devez indiquer, à l'aide du rapport, de quels objets il s'agit et demander d'autres informations sur les objets trouvés.



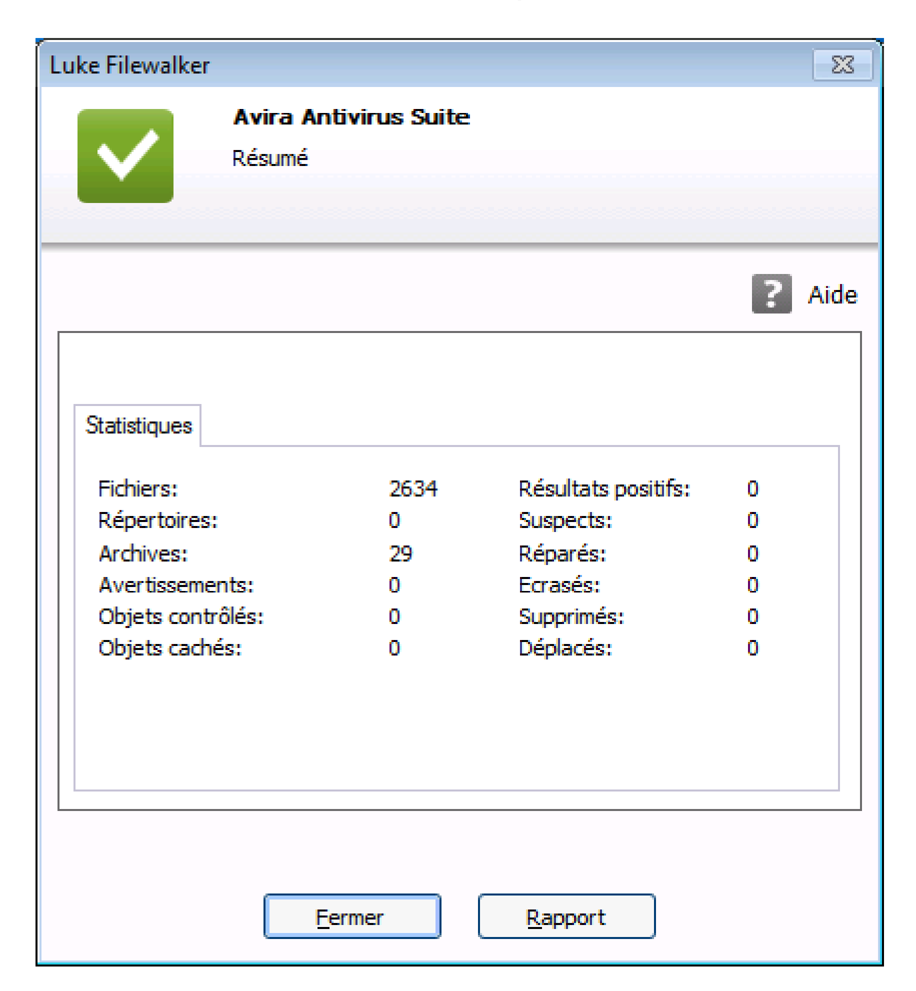
Boutons et liens

Bouton / Lien	Description
Informations sur les virus	En cliquant sur ce lien - quand la connexion Internet est active - vous arrivez sur une page Internet contenant des informations détaillées sur le virus ou le programme indésirable.
Aide	Cette page de l'aide en ligne est ouverte.
Arrêt	Le processus de contrôle est arrêté.
Pause	Le processus de contrôle est suspendu et peut être repris avec le bouton **Continuer**.
Continuer	Le processus de contrôle suspendu reprend.
Quitter	Le scanner se ferme.



Rapport	Le fichier rapport de la recherche s'affiche.

6.2.2 Luke Filewalker : statistiques de la recherche



Informations affichées : statistiques

Fichiers : nombre total de fichiers parcourus

Répertoires : nombre total de répertoires parcourus

Archive : nombre d'archives contrôlées

Avertissements : nombre de messages d'avertissement relatifs à des virus détectés

Objets contrôlés : nombre d'objets contrôlés lors de la recherche de rootkits

Objets cachés : nombre d'objets cachés qui ont été trouvés (rootkits)

Résultats positifs : nombre de virus et programmes indésirables trouvés

Suspects : nombre de fichiers signalés par l'heuristique

Réparés : nombre de fichiers réparés

Écrasés : nombre de fichiers écrasés

Supprimés : nombre de fichiers supprimés

Déplacés : nombre de fichiers déplacés en quarantaine

Boutons et liens

Bouton / Lien	Description
Aide	Cette page de l'aide en ligne est ouverte.
Fermer	La fenêtre de résumé est refermée.
Rapport	Le fichier rapport de la recherche s'affiche.

7. Control Center

7.1 Aperçu

Le Control Center sert de plate-forme centrale d'information, de configuration et de gestion. Outre les rubriques sélectionnables individuellement, vous y trouverez une multitude d'options qui peuvent être sélectionnées à partir de la barre de menus.

Barre de menus

La barre de menus comprend les fonctions suivantes :

Fichier

- Quitter (Alt+F4)

Affichage

- État
- Sécurité PC
  - Scanner
  - Protection temps réel
- Sécurité Internet
  - FireWall
  - Protection Web désactivée
  - Protection e-mail
- Protection mobile
  - Avira Free Android Security
- Administration
  - Quarantaine
  - Planificateur
  - Rapports
  - Événements
- Actualiser (F5)

Extras

- Contrôler les secteurs d'amorçage...
- Liste des menaces détectées...
- Télécharger le CD de secours
- Configuration (F8)

Mise à jour

- Démarrer mise à jour...
- Mise à jour manuelle...

Aide

- Sujets
- Aidez-moi
- Aide en ligne
- Forum
- Télécharger le manuel
- Gestion des licences
- Recommander le produit
- Envoyer un commentaire
- À propos de Avira Antivirus Suite

> **Remarque**
> La touche [**Alt**] permet d'activer la navigation au clavier dans la barre de menus. Si la navigation est activée, vous pouvez vous déplacer dans le menu à l'aide des touches fléchées. La touche Entrée vous permet d'activer la rubrique actuellement sélectionnée.

Rubriques

La barre de navigation de gauche comporte les rubriques suivantes :

- État

SÉCURITÉ PC

- Scanner
- Protection temps réel

SÉCURITÉ INTERNET

- FireWall
- Protection Web désactivée
- Protection e-mail

PROTECTION MOBILE

- Avira Free Android Security

ADMINISTRATION

- Quarantaine
- Planificateur
- Rapports
- Événements

Description des rubriques

- **État** : l'écran de démarrage **État** présente toutes les rubriques vous permettant de surveiller les fonctionnalités du programme (voir État).
  - La fenêtre **État** vous permet de voir d'un seul coup d'œil quels modules sont actifs et fournit des informations sur la dernière mise à jour effectuée.
- *SÉCURITÉ PC* : vous trouverez ici les composants vous permettant de contrôler l'absence de virus et de logiciels malveillants dans les fichiers de votre ordinateur.
  - La rubrique **Scanner** vous permet de configurer et de démarrer simplement la recherche directe (voir Scanner). Les profils prédéfinis permettent d'effectuer une recherche avec des options standard adaptées. À l'aide de la sélection manuelle (qui est enregistrée) ou en créant des profils personnalisés, vous pouvez également adapter la recherche de virus et de programmes indésirables à vos besoins personnels.
  - La rubrique Protection temps réel vous fournit des informations sur les fichiers contrôlés, ainsi que d'autres données statistiques, pouvant être réinitialisées à tout moment, et vous permet d'accéder au fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.
- *SÉCURITÉ INTERNET* : vous trouverez ici les composants vous permettant de protéger votre ordinateur contre les virus et logiciels malveillants provenant d'Internet et les accès réseau indésirables.
  - La rubrique Protection Web vous fournit des informations sur les URL contrôlées et les virus trouvés, ainsi que d'autres données statistiques qu'il est possible de réinitialiser à tout moment, et vous permet d'afficher le fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.
  - La rubrique **Protection e-mail** vous indique les e-mails contrôlés par ce service, leurs propriétés ainsi que d'autres données statistiques. (voir Protection e-mail).
- *PROTECTION MOBILE* : la catégorie Avira Free Android Security vous permet d'accéder en ligne à vos appareils Android.
  - Avira Free Android Security vous permet de gérer tous vos appareils dotés d'un système d'exploitation Android.
- *ADMINISTRATION* : vous trouverez ici des outils vous permettant d'isoler et de gérer les fichiers suspects ou infectés par des virus ainsi que de planifier des tâches récurrentes.

- Sous la rubrique **Quarantaine** se trouve le gestionnaire de quarantaines. Il s'agit de l'emplacement central pour les fichiers déjà en quarantaine ou pour les fichiers suspects que vous souhaitez mettre en quarantaine (voir Quarantaine). En outre, vous avez la possibilité d'envoyer un fichier par e-mail à l'Avira Malware Research Center.
- La rubrique **Planificateur** vous permet de créer des tâches de contrôle et de mise à jour programmées ainsi que des tâches de sauvegarde et d'adapter ou de supprimer les tâches existantes (voir Planificateur).
- La rubrique **Rapports** vous permet de visualiser les résultats des actions effectuées (voir Rapports).
- La rubrique **Événements** vous permet de vous informer sur les événements générés par les modules du programme (voir Événements).

Boutons et liens

Les boutons et les liens suivants sont disponibles.

Bouton / Lien	Commande clavier	Description
Configuration		La boîte de dialogue de configuration correspondant à la rubrique s'affiche à l'écran.
	F1	Le thème de l'aide en ligne correspondant s'affiche à l'écran.

7.2 Fichier

7.2.1 Quitter

La rubrique **Quitter** du menu **Fichier** permet de fermer le Control Center.

7.3 Affichage

7.3.1 État

L'écran de démarrage **État** du Control Center permet de voir d'un seul coup d'œil si votre système est protégé et quels modules d'Avira sont actifs. En outre, la fenêtre **État** fournit des informations concernant la dernière mise à jour effectuée. Vous voyez par ailleurs si vous disposez d'une licence valide.

- Sécurité PC : Protection temps réel, Dernière recherche, Dernière mise à jour, Votre produit est activé
- Sécurité Internet : Protection Web, Protection e-mail, FireWall,, Mode jeu,

> **Remarque**
> Le contrôle de compte d'utilisateur (UAC) a besoin de votre accord pour activer ou désactiver les services Protection temps réel, FireWall, Protection Web et Protection e-mail dans les systèmes d'exploitation à partir de Windows Vista.

Sécurité PC

Cette zone contient des informations sur l'état actuel des services et fonctions de protection qui protègent localement votre ordinateur des virus et logiciels malveillants.

Protection temps réel

Cette zone contient des informations sur l'état actuel de la protection temps réel.

Le bouton **Activé/Désactivé** permet d'activer et de désactiver la protection temps réel. Cliquez sur la barre de navigation **Protection temps réel** pour accéder à des options supplémentaires. Vous recevez en outre des informations quant à l'état des derniers logiciels malveillants détectés et des fichiers infectés. Cliquez sur **Configuration** afin de pouvoir définir des paramètres supplémentaires.

- **Configuration** : vous accédez à la configuration où vous pouvez définir des paramètres pour les composants du module de protection temps réel.

Les possibilités suivantes s'offrent à vous :

Icône	État	Option	Description
✅	*Activé*	**Désactiver**	Le service Protection temps réel est actif, votre système est donc contrôlé en permanence quant à l'absence de virus et de programmes indésirables. **Remarque** Vous pouvez désactiver le service Protection temps réel. Notez toutefois que si ce service est désactivé, vous n'êtes plus protégé contre les virus et programmes indésirables. Tous les fichiers peuvent passer dans le système sans entrave et provoquer éventuellement des dégâts.
❗	*Désactivé*	**Activer**	Le service Protection temps réel est désactivé, ce qui signifie que le service est chargé mais inactif. **Avertissement** Il n'y a pas de recherche de virus et de programmes indésirables. Tous les fichiers peuvent passer dans le système sans entrave. Vous n'êtes pas protégé contre les virus et programmes indésirables. **Remarque** Pour être de nouveau protégé contre les virus et programmes indésirables, cliquez sur le bouton **Activé/Désactivé** situé en regard du service Protection temps réel dans la zone Sécurité PC de la fenêtre d'état.

	Service arrêté	**Démarrer**	Le service Protection temps réel est arrêté. **Avertissement** Il n'y a pas de recherche de virus et de programmes indésirables. Tous les fichiers peuvent passer dans le système sans entrave. Vous n'êtes pas protégé contre les virus et programmes indésirables. **Remarque** Pour être de nouveau protégé contre les virus et programmes indésirables, cliquez sur le bouton **Activé/Désactivé**. L'état actuel doit maintenant afficher *Activé*.
	Inconnu	**Aide**	Cet état s'affiche en présence d'une erreur inconnue. Dans ce cas, veuillez vous adresser à notre Support.

Dernière recherche

Cette zone contient des informations sur le dernier contrôle du système effectué. En cas de contrôle intégral du système, tous les disques durs de votre ordinateur sont entièrement contrôlés. Dans ce cadre, tous les processus de recherche et de contrôle sont utilisés, à l'exception du contrôle d'intégrité des fichiers système : recherche standard sur les fichiers, contrôle du Registre et des secteurs d'amorçage, recherche de rootkits et de logiciels malveillants actifs, etc.

Est visible :

- la date du dernier contrôle intégral du système

Les possibilités suivantes s'offrent à vous :

Contrôle du système	Option	Description
Non exécutée	**Contrôler le système**	Depuis l'installation, aucun contrôle intégral du système n'a été exécuté. **Avertissement** Le système n'est pas contrôlé. Il est possible que des virus et programmes indésirables se trouvent sur votre ordinateur. **Remarque** Pour contrôler votre ordinateur, cliquez sur le bouton Contrôler le système.
Date du dernier contrôle du système, par ex. *18/09/2011*	**Contrôler le système**	Vous avez effectué un contrôle intégral du système à la date indiquée. **Remarque** Nous vous conseillons d'utiliser la tâche de contrôle standard *Contrôle intégral du système* : activez cette tâche de contrôle dans le planificateur.
Inconnu	**Aide**	Cet état s'affiche en présence d'une erreur inconnue. Dans ce cas, veuillez vous adresser à notre Support.

Dernière mise à jour

Cette zone contient des informations sur l'état actuel de votre dernière mise à jour effectuée.

Est visible :

- la date de la dernière mise à jour
  - Cliquez sur le bouton Configuration afin de pouvoir définir des paramètres supplémentaires pour la mise à jour automatique.



Les possibilités suivantes s'offrent à vous :

Icône	État	Option	Description
✅	Date de la dernière actualisation, par ex. *18/07/2011*	**Démarrer mise à jour**	Le programme a été actualisé dans les dernières 24 heures. **Remarque** Le bouton Démarrer mise à jour vous permet d'obtenir la version la plus récente de votre produit Avira.
!	Date de la dernière actualisation, par ex. *15/07/2011*	**Démarrer mise à jour**	Depuis l'actualisation, 24 heures se sont déjà écoulées, mais vous vous trouvez encore dans le cycle de rappel de mise à jour que vous avez sélectionné. Celui-ci dépend des paramètres définis dans la Configuration. **Remarque** Le bouton Démarrer mise à jour vous permet d'obtenir la version la plus récente de votre produit Avira.

	Non exécutée	**Démarrer mise à jour**	Depuis l'installation, aucune mise à jour n'a encore été effectuée ou le cycle de rappel de mise à jour que vous avez sélectionné a été dépassé (voir Configuration) et aucune actualisation n'a été effectuée ou le fichier de définitions des virus est plus ancien que le cycle de rappel de mise à jour que vous avez sélectionné (voir Configuration). **Remarque** Le bouton **Démarrer mise à jour** vous permet d'obtenir la version la plus récente de votre produit Avira.
		Impossible	Les mises à jour ne sont pas possibles si la licence est périmée.

Votre produit est activé

Cette zone contient des informations sur l'état actuel de votre licence.

Les possibilités suivantes s'offrent à vous :

Version intégrale

Icône	État	Option	Signification
✅	Date de validité de la licence actuelle pour une version intégrale, par ex. *31/10/2011*	**Renouveler**	Vous disposez d'une licence valide pour votre produit Avira. Le bouton Renouveler permet d'accéder à la boutique en ligne d'Avira. Vous avez la possibilité d'y adapter votre licence actuelle à vos besoins et d'effectuer une mise à niveau vers Avira Premium.
!	Date de validité de la licence actuelle pour une version intégrale, par ex. *31/10/2011*	**Renouveler**	Vous disposez d'une licence valide pour votre produit Avira. La période restante de validité de la licence se limite toutefois à 30 jours, voire moins. Le bouton **Renouveler** permet d'accéder à la boutique en ligne d'Avira. Vous avez la possibilité d'y prolonger votre licence actuelle.
⚠	La licence a expiré le : *31/08/2011* par ex.	**Acheter**	Votre licence pour votre produit Avira a expiré. Le bouton **Acheter** permet d'accéder à la boutique en ligne d'Avira. Vous avez la possibilité d'y acheter une licence actuelle. **Avertissement** Les mises à jour ne sont plus possibles si votre licence est périmée. Les fonctions de protection du programme sont désactivées et ne peuvent plus être activées.

Licence d'évaluation

Icône	État	Option	Signification
	Date de validité de la licence d'évaluation, par ex. *31/10/2011*	**Acheter**	Vous disposez d'une licence d'évaluation et avez ainsi la possibilité de tester l'intégralité des fonctions de votre produit Avira sur une période définie. Le bouton **Acheter** permet d'accéder à la boutique en ligne d'Avira. Vous avez la possibilité d'y acheter une licence actuelle.
	Date de validité de la licence d'évaluation, par ex. *31/10/2011*	**Renouveler**	Vous disposez d'une licence d'évaluation. La période restante de validité de la licence se limite toutefois à 30 jours, voire moins. Le bouton **Renouveler** permet d'accéder à la boutique en ligne d'Avira. Vous avez la possibilité d'y acheter une licence actuelle.
	La licence d'évaluation a expiré le : *31/08/2011*	**Acheter**	Votre licence pour votre produit Avira a expiré. Le bouton **Acheter** permet d'accéder à la boutique en ligne d'Avira. Vous avez la possibilité d'y acheter une licence actuelle. **Avertissement** Les mises à jour ne sont plus possibles si votre licence est périmée. Les fonctions de protection du programme sont désactivées et ne peuvent plus être activées.

Sécurité Internet

Cette zone contient des informations sur l'état actuel des services qui protègent votre ordinateur des virus et logiciels malveillants en provenance d'Internet.

- **FireWall** : ce service contrôle les voies de communication en provenance et à destination de votre ordinateur.

- **Protection Web** : ce service contrôle les données transférées lors de la navigation sur Internet et téléchargées dans votre navigateur Web (surveillance des ports 80, 8080, 3128).
- **Protection e-mail** : ce service vérifie l'absence de virus et de logiciels malveillants dans les e-mails et leurs pièces jointes.
- **Mode jeu** : si l'option est activée, votre produit Avira bascule automatiquement dans le mode jeu lorsqu'une application est affichée en plein écran sur votre ordinateur. Voir Mode jeu.

D'autres options relatives à ces services sont disponibles dans un menu contextuel lorsque vous cliquez sur le bouton **Configuration** à côté de l'option **Activé/Désactivé** :

- **Configuration** : vous accédez à la configuration où vous pouvez définir des paramètres pour les composants du service.

Les possibilités suivantes s'offrent à vous : *Services*

Icône	État	État de service	Option	Signification
✅	*OK*	Activé	**Désactiver**	Tous les services de sécurité Internet sont activés. **Remarque** Vous pouvez désactiver un service en cliquant sur le bouton **Activé/Désactivé**. Notez toutefois que si un service est désactivé, vous n'êtes plus totalement protégé contre les virus et logiciels malveillants.
!	*Restreint*	Désactivé	**Activer**	Un service est désactivé ; le service est donc démarré mais inactif. **Avertissement** Votre système n'est pas totalement surveillé. Il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. **Remarque** Pour activer le service, cliquez sur le bouton**Activé/Désactivé** en regard du service correspondant.

	Avertissement	Service arrêté	**Démarrer**	Un service a été arrêté. **Avertissement** Votre système n'est pas totalement surveillé. Il est possible que des virus et programmes indésirables arrivent sur votre ordinateur. **Remarque** Pour démarrer le service et faire surveiller votre système, cliquez sur le bouton **Activé/Désactivé**. Le service est démarré et activé.
		Inconnu	**Aide**	Cet état s'affiche en présence d'une erreur inconnue. Dans ce cas, veuillez vous adresser à notre Support.

7.3.2 Mode jeu

Si vous exécutez sur votre ordinateur des applications qui nécessitent le mode plein écran, vous pouvez bloquer de manière ciblée les notifications de Bureau et avertissements, tels que les fenêtres contextuelles et les alertes concernant les produits, en activant le mode jeu.

Un clic sur le bouton **Activé/Désactivé** vous permet d'activer le mode jeu ou de définir le mode automatique. Par défaut, le mode jeu est configuré avec l'option **automatique** et est représenté en vert. Ce paramètre par défaut permet à votre produit Avira de basculer automatiquement dans le mode jeu lorsqu'une application est affichée en plein écran.

- Cliquez sur le bouton à gauche à côté de **Désactivé**, pour activer le mode jeu.
  - ↳ Le mode jeu est activé et le bouton s'affiche en jaune.

> **Remarque**
> Nous vous conseillons de ne modifier que temporairement le statut prédéfini **Désactivé** avec sa détection automatique d'applications en plein écran, car, en mode jeu, les notifications de Bureau et les avertissements ne s'affichent pas pour vous signaler les accès au réseau et les dangers éventuels.

7.3.3 Scanner Système

La rubrique **Scanner** vous permet de configurer et de démarrer simplement la recherche directe, c'est-à-dire la recherche sur demande. Les profils prédéfinis permettent d'effectuer une recherche avec des options standard adaptées. Il est également possible, à l'aide de la sélection manuelle ou en créant des profils personnalisés, d'ajuster à vos besoins la recherche de virus et de programmes indésirables. L'action souhaitée est accessible en sélectionnant l'icône dans la barre d'outils, via une commande clavier ou encore via le menu contextuel. Démarrez la recherche via la rubrique Démarrer la recherche avec le profil choisi.

L'affichage et l'utilisation des profils éditables sont les mêmes que dans Windows Explorer. Chaque dossier du répertoire principal correspond à un profil. Les dossiers et fichiers à parcourir sont signalés par une coche devant le dossier ou le fichier en question ou peuvent l'être.

- Pour changer de répertoire, cliquez deux fois sur le répertoire souhaité.
- Pour changer de lecteur, cliquez deux fois sur la lettre du lecteur souhaité.
- Pour sélectionner des dossiers et lecteurs, vous pouvez cliquer sur la case devant le symbole du dossier ou du lecteur, ou effectuer la sélection via le menu contextuel.
- La barre de défilement et les flèches de défilement vous permettent de naviguer dans la structure du menu.

Profils prédéfinis

Vous disposez de profils prédéfinis pour vos recherches.

> **Remarque**
> Ces profils sont protégés en écriture et ne peuvent pas être modifiés ni supprimés. Pour adapter un profil à vos besoins, sélectionnez, pour une recherche unique, le dossier Sélection manuelle ou Créer un nouveau profil pour créer un profil personnalisé, qui peut être enregistré.
>
> **Remarque**
> Les options de recherche des profils prédéfinis peuvent être définies sous Configuration > Scanner > Recherche > Fichiers. Vous pouvez adapter ces paramètres à vos besoins.

Lecteurs locaux

Tous les lecteurs locaux de votre système sont parcourus à la recherche de virus et de programmes indésirables.

Disques durs locaux

Tous les disques durs locaux de votre système sont parcourus à la recherche de virus et de programmes indésirables.

Lecteurs amovibles

Tous les lecteurs amovibles de votre système sont parcourus à la recherche de virus et de programmes indésirables.

Répertoire système Windows

Le répertoire système Windows de votre système est parcouru à la recherche de virus et de programmes indésirables.

Contrôle intégral du système

Tous les disques durs locaux de votre ordinateur sont parcourus à la recherche de virus et de programmes indésirables. Dans ce cadre, tous les processus de recherche et de contrôle sont utilisés, à l'exception du contrôle d'intégrité des fichiers système : recherche standard sur les fichiers, contrôle du registre et des secteurs d'amorçage, recherche de rootkits, etc. (voir Scanner > Aperçu). Les processus de contrôle sont effectués indépendamment des paramètres du scanner dans la configuration sous Scanner > Recherche : autres paramètres.

Contrôle rapide du système

Les dossiers les plus importants de votre système (répertoires *Windows*, *Programmes*, *Documents et paramètres\Default User*, *Documents et paramètres\All Users*) sont parcourus à la recherche de virus et de programmes indésirables.

Mes documents

L'emplacement par défaut « *Mes documents* » de l'utilisateur connecté est parcouru à la recherche de virus et de programmes indésirables.

> **Remarque**
> Sous Windows, le répertoire « *Mes documents* » se trouve dans le profil de l'utilisateur et est utilisé comme emplacement par défaut pour les documents enregistrés. Dans la configuration par défaut, le répertoire se trouve sous *C:\Documents et paramètres\[Nom d'utilisateur]\Mes documents*.

Processus actifs

Tous les processus en cours sont parcourus à la recherche de virus et de programmes indésirables.

Détection de rootkits et logiciels malveillants actifs

L'ordinateur est parcouru à la recherche de rootkits et de logiciels malveillants actifs (en fonctionnement). Tous les processus en cours sont contrôlés.

> **Remarque**
> En mode interactif, vous avez le choix du traitement des résultats positifs. En mode automatique, les résultats positifs sont consignés dans le fichier rapport.

> **Remarque**
> La recherche de rootkits n'est pas disponible sous Windows XP 64 bits.

7.3.4 Sélection manuelle

Si vous souhaitez adapter la recherche à vos besoins, sélectionnez ce dossier. Sélectionnez les répertoires et fichiers à parcourir.

> **Remarque**
> Le profil **Sélection manuelle** sert à parcourir les données sans avoir à créer un autre profil.

Profils personnalisés

La création d'un profil est possible via la barre d'outils, via une commande clavier ou encore via le menu contextuel.

Les nouveaux profils peuvent être enregistrés sous le nom que vous souhaitez et utilisés lors de la recherche à commande manuelle pour la création de recherches programmées à l'aide du planificateur.

Barre d'outils et commandes clavier

Icône	Commande clavier	Description
	F3	**Démarrer la recherche avec le profil choisi** Le profil sélectionné est parcouru à la recherche de virus et de programmes indésirables.
	F6	**Démarrer la recherche avec le profil choisi en tant qu'administrateur** Le profil sélectionné est parcouru avec les droits d'administrateur.
	Inser	**Créer un nouveau profil** Un profil est créé.
	F2	**Renommer le profil sélectionné** Donne le nom que vous avez choisi au profil sélectionné.
	F4	**Créer un raccourci sur le Bureau pour le profil sélectionné** Crée un raccourci pour le profil sélectionné sur le Bureau.
	Suppr	**Supprimer le profil sélectionné** Le profil sélectionné est définitivement supprimé.

Menu contextuel

Vous accédez au menu contextuel de cette rubrique en sélectionnant le profil souhaité avec la souris et en maintenant le bouton droit de la souris enfoncé.

Démarrer la recherche

Le profil sélectionné est parcouru à la recherche de virus et de programmes indésirables.

Démarrer la recherche (administrateur)

(Cette fonction n'est disponible que depuis Windows Vista. Pour exécuter cette action, les droits d'administrateur sont nécessaires.)

Le profil sélectionné est parcouru à la recherche de virus et de programmes indésirables.

Créer un nouveau profil

Un profil est créé. Sélectionnez les répertoires et fichiers à contrôler.

Renommer le profil

Donne le nom que vous avez choisi au profil sélectionné.

> **Remarque**
> Cette entrée n'est pas sélectionnable dans le menu contextuel si un profil prédéfini est sélectionné.

Supprimer le profil

Le profil sélectionné est définitivement supprimé.

> **Remarque**
> Cette entrée n'est pas sélectionnable dans le menu contextuel si un profil prédéfini est sélectionné.

Filtre fichier

Standard :

Signifie que les fichiers sont contrôlés en fonction du paramètre du groupe Fichiers de la configuration. Vous pouvez adapter ce paramètre à vos besoins dans la configuration. Vous accédez à la configuration via le bouton ou le lien Configuration.

Recherche sur tous les fichiers :

Tous les fichiers sont vérifiés sans tenir compte du paramètre de la configuration.

Personnalisé :

Vous accédez à une fenêtre de dialogue, où figurent toutes les extensions de fichiers concernés par une recherche. Les extensions proposées sont des entrées standard. Il est toutefois possible d'ajouter ou de supprimer des entrées.

> **Remarque**
> Cette entrée du menu contextuel n'est sélectionnable que si la souris se trouve au-dessus d'une case à cocher.
> La sélection de l'option n'est pas possible avec les profils prédéfinis.

Sélectionner

Avec les sous-répertoires :

tout est contrôlé dans le nœud sélectionné (coche noire).

Sans sous-répertoires :

seuls les fichiers sont contrôlés dans le nœud sélectionné (coche verte).

Uniquement les sous-répertoires :

dans le nœud sélectionné, seuls les sous-répertoires sont contrôlés, et non les fichiers se trouvant dans le nœud (coche grise, les sous-répertoires ont une coche noire).

Aucune sélection :

la sélection est supprimée, le nœud sélectionné n'est pas contrôlé (pas de coche).

Remarque
Cette entrée du menu contextuel n'est sélectionnable que si la souris se trouve au-dessus d'une case à cocher.
La sélection de l'option n'est pas possible avec les profils prédéfinis.

Créer un raccourci bureau

Crée un raccourci pour le profil sélectionné sur le bureau.

Remarque
Cette entrée n'est pas sélectionnable dans le menu contextuel si le profil Sélection manuelle est sélectionné, car les paramètres de la sélection manuelle ne peuvent pas être enregistrés définitivement.

7.3.5 Protection temps réel

La rubrique **Protection temps réel** vous fournit des informations sur les fichiers contrôlés, ainsi que d'autres données statistiques, pouvant être réinitialisées à tout moment, et vous permet d'accéder au fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.

Remarque
Si le service Protection temps réel n'est pas démarré, le bouton en regard du module s'affiche en jaune. Vous pouvez toutefois afficher le fichier rapport de la protection temps réel.

Barre d'outils

Icône	Description
	Afficher le fichier rapport Le fichier rapport de la protection temps réel s'affiche.
	Réinitialiser les données statistiques Les informations statistiques de cette rubrique sont mises à zéro.

Informations affichées

Dernier fichier infecté

Indique le nom et l'emplacement du dernier fichier trouvé par la protection temps réel.

Dernier logiciel malveillant trouvé

Nomme le dernier virus ou programme indésirable trouvé.

Icône	Description
Informations sur les virus	En cliquant sur l'icône ou le lien, vous obtenez des informations détaillées sur le virus ou le programme indésirable, dès lors qu'une connexion Internet active est disponible.

Dernier fichier contrôlé

Indique le nom et le chemin du dernier fichier contrôlé par la protection temps réel.

Statistiques

Nombre de fichiers

Indique le nombre de fichiers contrôlés jusqu'ici.

Nombre de logiciels malveillants trouvés

Indique le nombre de virus et programmes indésirables trouvés jusqu'à présent.

Nombre de fichiers suspects

Indique le nombre de fichiers signalés par l'heuristique.

Nombre de fichiers supprimés

Indique le nombre des fichiers supprimés jusqu'ici.

Nombre de fichiers réparés

Indique le nombre de fichiers réparés jusqu'ici.

Nombre de fichiers déplacés

Indique le nombre de fichiers déplacés jusqu'ici.

Nombre de fichiers renommés

Indique le nombre de fichiers renommés jusqu'ici.

7.3.6 FireWall

Pare-feu Windows (à partir de Windows 7)

À partir de Windows 7, vous avez la possibilité de régler Pare-feu Windows à l'aide du centre de contrôle et de configuration.

La rubrique FireWall vous permet de contrôler l'état de Pare-feu Windows et de restaurer les paramètres recommandés en cliquant sur le bouton **Résoudre le problème**.

7.3.7 Protection Web

La rubrique **Protection Web** vous fournit des informations sur les URL contrôlées, ainsi que des données statistiques, pouvant être réinitialisées à tout moment, et vous permet d'accéder au fichier rapport. Des informations plus détaillées sur le dernier virus ou programme indésirable trouvé sont disponibles en un clic.

Barre d'outils

Icône	Description
	Afficher le fichier rapport Le fichier rapport de la protection Web s'affiche.
	Réinitialiser les données statistiques Les informations statistiques de cette rubrique sont mises à zéro.

Informations affichées

Dernière URL concernée

Indique la dernière URL trouvée par la protection Web.

Dernier virus ou programme indésirable trouvé

Nomme le dernier virus ou programme indésirable trouvé.

Icône/Lien	Description
Informations sur les virus	En cliquant sur l'icône ou le lien, vous obtenez des informations détaillées sur le virus ou le programme indésirable, dès lors qu'une connexion Internet active est disponible.

Dernière URL contrôlée

Indique le nom et le chemin de la dernière URL contrôlée par la protection Web.

Statistiques

Nombre d'URL contrôlées

Indique le nombre d'URL contrôlées jusqu'à présent.

Nombre de messages

Indique le nombre de virus et programmes indésirables trouvés jusqu'à présent.

Nombre d'URL bloquées

Indique le nombre d'URL bloquées jusqu'à présent.

Nombre d'URL ignorées

Indique le nombre d'URL ignorées jusqu'à présent.

7.3.8 Protection e-mail

La rubrique **Protection e-mail** vous indique les e-mails contrôlés par ce service, leurs propriétés ainsi que d'autres données statistiques.

> **Remarque**
> Si le service Protection e-mail n'est pas lancé, le bouton en regard du module s'affiche en jaune. Il reste toutefois possible d'afficher le fichier rapport de la protection e-mail. Si ce service n'est pas disponible dans votre produit Avira, le bouton est grisé.

> **Remarque**
> L'exclusion de certaines adresses e-mail du contrôle concernant les logiciels malveillants ne s'applique évidemment qu'aux e-mails entrants. Pour désactiver le contrôle des e-mails sortants, désactivez cette fonction dans la configuration sous Protection e-mail > Recherche.

Barre d'outils

Icône	Description
	Afficher le fichier rapport Le fichier rapport de la protection e-mail s'affiche.
	Afficher les propriétés de l'e-mail sélectionné Ouvre une fenêtre de dialogue avec des informations détaillées sur l'e-mail sélectionné.
	Ne plus contrôler l'absence de logiciel malveillant pour cette adresse e-mail L'adresse e-mail sélectionnée ne fera plus l'objet de recherche de virus et de programmes indésirables. Vous pouvez annuler ce paramètre dans la configuration sous **Protection e-mail > Généralités > Exceptions** (voir Exceptions).
	Supprimer les e-mails sélectionnés L'e-mail sélectionné est supprimé de la mémoire tampon. Le fichier reste toutefois dans votre programme de messagerie électronique.
	Réinitialiser les données statistiques Les informations statistiques de cette rubrique sont mises à zéro.

E-mails contrôlés

Cette zone affiche les e-mails contrôlés par le service Protection e-mail.

Icône	Description
	Aucun virus ou programme indésirable n'a été trouvé.
	Un virus ou programme indésirable a été trouvé.

Type

Affiche le protocole utilisé pour recevoir l'e-mail ou pour l'envoyer :

- POP3 : e-mail reçu via POP3
- IMAP : e-mail reçu via IMAP
- SMTP : e-mail envoyé via SMTP

Expéditeur/Destinataire

Indique l'adresse de l'expéditeur de l'e-mail.

Objet

Indique l'objet de l'e-mail reçu.

Date/Heure

Indique quand la présence de spam a été contrôlée sur l'e-mail.

> **Remarque**
> Si vous souhaitez avoir plus d'informations sur un e-mail, cliquez deux fois sur celui-ci.

Statistiques

Action e-mail

Indique l'action effectuée lorsque le service Protection e-mail trouve un virus ou un programme indésirable dans un e-mail. En mode interactif, aucun affichage n'est disponible ici, car vous pouvez choisir vous-même la procédure à effectuer en cas de résultat positif.

> **Remarque**
> Vous pouvez adapter ce paramètre à vos besoins dans la configuration. Vous accédez à la configuration via le bouton ou le lien Configuration.

Pièces jointes concernées

Indique l'action effectuée lorsque le service Protection e-mail trouve un virus ou un programme indésirable dans une pièce jointe concernée. En mode interactif, aucun affichage n'est disponible ici, car vous pouvez choisir vous-même la procédure à effectuer en cas de résultat positif.

> **Remarque**
> Vous pouvez adapter ce paramètre à vos besoins dans la configuration. Vous accédez à la configuration via le bouton ou le lien Configuration.

Nombre d'e-mails

Indique le nombre d'e-mails parcourus par la protection e-mail.

Dernier message

Nomme le dernier virus ou programme indésirable trouvé.

Nombre de messages

Indique le nombre de virus et programmes indésirables trouvés et signalés jusqu'à maintenant.

E-mails suspects

Indique le nombre d'e-mails signalés par l'heuristique.

Nombre d'e-mails reçus

Indique le nombre d'e-mails reçus.

Nombre d'e-mails envoyés

Indique le nombre d'e-mails envoyés.

7.3.9 Avira Free Android Security

Avira Free Android Security est une application visant à empêcher la perte et/ou le vol de votre appareil. Cette application propose des fonctions vous permettant de retrouver votre appareil mobile si vous l'avez égaré ou pire : s'il vous a été volé. En outre, cette application vous permet de bloquer des appels ou SMS entrants. Avira Free Android Security protège les téléphones mobiles et smartphones dotés d'un système d'exploitation Android.

Avira Free Android Security comprend deux composants :

- L'application proprement dite, installée sur votre appareil Android
- La console Web Avira Android pour l'enregistrement et le contrôle des fonctionnalités

Avira Free Android Security est une application gratuite pour laquelle aucune licence n'est nécessaire. Avira Free Android Security prend en charge les marques les plus répandues, telles que Samsung, HTC, LG et Motorola.

Vous trouverez de plus amples informations sur notre site Web :

www.avira.com/android

7.3.10 Quarantaine

Le **gestionnaire de quarantaines** administre les objets affectés (fichiers et e-mails). Votre produit Avira peut déplacer les objets affectés dans un format spécial dans le répertoire de quarantaine. Ils ne peuvent alors plus être exécutés ni ouverts.

> **Remarque**
> Pour déplacer les objets dans le gestionnaire de quarantaines, sélectionnez l'option correspondante pour la quarantaine dans la **Configuration** sous **Scanner** et **Protection temps réel** ainsi que **Protection e-mail**, respectivement sous **Recherche > Action si résultat positif** lorsque vous travaillez en **mode automatique**.
> En **mode interactif**, vous pouvez également sélectionner l'option correspondante pour la quarantaine.

Barre d'outils, commande clavier et menu contextuel

Icône	Commande clavier	Description
	F2	**Rechercher à nouveau les objets** Un objet sélectionné est de nouveau contrôlé à la recherche de virus et de programmes indésirables. Dans ce cadre, les paramètres de la recherche directe sont utilisés (voir Scanner).
	Entrée	**Propriétés** Ouvre une fenêtre de dialogue comportant des informations détaillées sur l'objet sélectionné. **Remarque** Les informations détaillées sont également accessibles en double-cliquant sur un objet.

(Windows Vista)	**F3**	**Restaurer les objets** Un objet sélectionné est restauré. Ensuite, l'objet se retrouve à son emplacement d'origine. **Remarque** Cette option n'est pas disponible pour les objets de type E-mail. **Avertissement** Les virus et programmes indésirables peuvent causer des dégâts considérables sur le système . Lorsque vous restaurez des fichiers, veillez à ne restaurer que ceux qui ont pu être nettoyés au cours d'une nouvelle recherche. **Remarque** Sous Windows Vista, la restauration d'objets n'est possible qu'avec les droits d'administrateur.
	F6	**Restaurer les objets à l'emplacement...** Un objet sélectionné peut être restauré à l'emplacement que vous souhaitez. Si vous choisissez cette option, une boîte de dialogue « Enregistrer sous » s'affiche et vous pouvez sélectionner l'emplacement pour l'enregistrement. **Avertissement** Les virus et programmes indésirables peuvent causer des dégâts considérables sur le système . Lorsque vous restaurez des fichiers, veillez à ne restaurer que ceux qui ont pu être nettoyés au cours d'une nouvelle recherche.

+	Inser	**Déplacer le fichier en quarantaine** Si un fichier vous semble suspect, cette option permet de l'ajouter manuellement au gestionnaire de quarantaines. Le cas échéant, téléchargez le fichier sur un serveur Web de l'Avira Malware Research Center, en vue d'un contrôle, à l'aide de l'option Envoyer l'objet.
	F4	**Envoyer les objets** L'objet est téléchargé sur un serveur Web de l'Avira Malware Research Center en vue d'un contrôle. Lorsque vous cliquez sur le bouton **Envoyer les objets**, une boîte de dialogue s'ouvre d'abord avec un formulaire de saisie de vos coordonnées. Indiquez les données complètes. Sélectionnez un type : **Fichier suspect** ou **Fausse alerte**. Cliquez sur **OK** pour télécharger le fichier suspect. **Remarque** La taille des fichiers que vous téléchargez est limitée à 20 Mo au format non compressé ou à 8 Mo en format compressé. **Remarque** Vous ne pouvez télécharger qu'un seul fichier à la fois.
✕	Suppr	**Supprimer les objets** Un fichier sélectionné est supprimé du gestionnaire de quarantaines. Le fichier ne peut pas être restauré.
	F7	**Exporter toutes les propriétés** Les propriétés de l'objet en quarantaine sélectionné sont exportées sous forme de fichier texte.
	F10	**Ouvrir le répertoire de quarantaine** Ouvre le dossier INFECTED.

> **Remarque**
> Vous avez la possibilité d'exécuter des actions pour plusieurs objets sélectionnés.
> Pour sélectionner plusieurs objets, maintenez la touche Ctrl ou Maj (sélection d'objets situés les uns sous les autres) enfoncée pendant la sélection des objets dans le gestionnaire de quarantaines. Pour sélectionner tous les objets affichés, appuyez sur **Ctrl + A**
> . Pour l'action **Afficher les propriétés**, la sélection de plusieurs objets est impossible. La sélection multiple n'est pas non plus possible pour l'action **Envoyer les objets**, car un seul fichier peut être téléchargé à la fois.

Tableau

Statut

Un objet en quarantaine peut avoir divers états :

Icône	Description
✅	Aucun virus ni programme indésirable n'a été trouvé, l'objet est « propre ».
⚠	Un virus ou programme indésirable a été trouvé.
!	Si un fichier suspect a été ajouté au gestionnaire de quarantaines via l'option Déplacer le fichier en quarantaine, il reçoit ce symbole de remarque.

Type

Désignation	Description
E-mail	L'objet trouvé est un e-mail.
Fichier	L'objet trouvé est un fichier.

Détection

Affiche le nom du logiciel malveillant détecté.
Les résultats positifs de l'heuristique sont repérés par l'abréviation HEUR/.

Source

Indique le chemin où l'objet a été trouvé.

Date/Heure

Indique la date et l'heure du résultat positif.

Informations détaillées

Nom du fichier

Chemin complet et nom de fichier de l'objet

Objet en quarantaine

Nom de fichier de l'objet en quarantaine

Restauré

OUI / NON

OUI : l'objet sélectionné a été restauré.

NON : l'objet sélectionné n'a pas été restauré.

Téléchargé vers Avira

OUI / NON

OUI : l'objet a été téléchargé sur un serveur Web de l'Avira Malware Research Center

en vue d'un contrôle.

NON : l'objet n'a pas encore été téléchargé sur un serveur Web de l'Avira Malware Research Center

en vue d'un contrôle.

Système d'exploitation

Station de travail Windows XP : le logiciel malveillant a été détecté par un produit de bureau Avira.

Moteur de recherche

Numéro de version du moteur de recherche

Fichier de définitions des virus

Numéro de version du fichier de définitions des virus

Détection

Nom du logiciel malveillant détecté

Date/Heure

Date et heure du résultat positif

7.3.11 Planificateur

Le **Planificateur** vous permet de créer des tâches de contrôle et de mise à jour planifiées et d'ajuster ou de supprimer des tâches existantes.

La tâche suivante est définie par défaut après l'installation :

- Tâche de contrôle **Contrôle rapide du système** (configuration par défaut) : un contrôle rapide du système est effectué automatiquement toutes les semaines. Lors du contrôle rapide du système, les fichiers et dossiers les plus importants de votre ordinateur sont parcourus à la recherche de virus ou de programmes indésirables. Vous pouvez modifier la tâche de contrôle ; nous vous conseillons toutefois de définir d'autres tâches de contrôle qui correspondent mieux à vos besoins.

Barre d'outils, commande clavier et menu contextuel

Icône	Commande clavier	Menu contextuel
+	Ins	**Ajouter une nouvelle tâche** Crée une nouvelle tâche. Un assistant vous guide au cours du processus de définition des paramètres nécessaires.
i	Entrée	**Propriétés** Ouvre une fenêtre de dialogue contenant des informations détaillées sur la tâche sélectionnée.
	F2	**Modifier la tâche** Ouvre l'assistant de création et de modification d'une tâche.
×	Suppr	**Supprimer la tâche** Supprime de la liste les tâches sélectionnées.

		Afficher le fichier rapport Le fichier rapport du planificateur s'affiche.
	F3	Démarrer la tâche Démarre une tâche sélectionnée dans la liste.
	F4	Arrêter la tâche Arrête une tâche démarrée et sélectionnée.

Tableau

Type de tâche

Icône	Description
	La tâche est une tâche de mise à jour.
	La tâche est une tâche de contrôle.

Nom

Désignation de la tâche.

Action

Indique s'il s'agit d'une **recherche** ou d'une **mise à jour**.

Fréquence

Indique à quelle fréquence et quand la tâche est démarrée.

Affichage de la fenêtre

Les modes d'affichage suivants sont disponibles :

- **Invisible :** la tâche est exécutée en arrière-plan et n'est pas visible. Cela s'applique aux tâches de contrôle et aux tâches de mise à jour.

  Réduit : la fenêtre des tâches n'affiche qu'une barre de progression.

  Agrandi : la fenêtre des tâches est complètement visible.

Activé

La tâche est activée avec l'activation de la case.

> **Remarque**
> Si la fréquence de la tâche est réglée sur **Immédiatement**, la tâche est démarrée aussitôt après l'activation. Cela vous permet de redémarrer la tâche en fonction de vos besoins.

État

Indique l'état de la tâche :

- **Prête** : la tâche est prête à être exécutée.

  En cours : la tâche a été démarrée et est en cours d'exécution.

Créer des tâches avec le planificateur

L'assistant de planification vous aide à planifier, configurer et créer

- une recherche programmée de virus et programmes indésirables
- une mise à jour programmée via Internet

Pour les deux types de tâches, vous devez indiquer

- le nom et la description de la tâche
- quand la tâche doit démarrer
- à quelle fréquence la tâche doit être exécutée
- le mode d'affichage de la fenêtre de la tâche

Fréquence de la tâche

Option	**Description**
Immédiatement	La tâche est démarrée dès que vous quittez l'assistant de planification.
Tous les jours	La tâche est démarrée tous les jours à une heure définie, par ex. à 22h00.

Toutes les semaines	La tâche démarre toutes les semaines, un jour particulier ou plusieurs jours de la semaine, à une heure définie, par ex. le mardi et le vendredi à 16h26.
Par intervalle	La tâche est exécutée à un intervalle défini, par ex. toutes les 24 heures.
Une fois	La tâche est exécutée une seule fois à un moment défini, par ex. le 10/04/04 à 10h04.
Connexion	La tâche est exécutée à chaque processus de connexion d'un utilisateur de Windows.

Moment de démarrage de la tâche

Vous pouvez définir un jour, une date, une heure ou un intervalle pour le moment de démarrage de la tâche. Ceci ne s'affiche pas si vous avez indiqué *Immédiatement* comme moment du démarrage.

Selon le type de tâche, il existe diverses options complémentaires :

Démarrer également la tâche quand une connexion Internet est établie

Outre la fréquence définie, la tâche est exécutée à chaque démarrage d'une connexion Internet.
Cette option est sélectionnable lors d'une tâche de mise à jour qui doit être exécutée tous les jours, toutes les semaines ou à intervalle régulier.

Rattraper la tâche quand la date est déjà passée

Le programme effectue les tâches antérieures qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.
Cette option est sélectionnable lors d'une tâche de mise à jour ou de contrôle qui doit être effectuée tous les jours, toutes les semaines ou à intervalle régulier.

Arrêter l'ordinateur quand la tâche a été exécutée

L'ordinateur est arrêté, une fois la tâche exécutée et achevée. Cette option est disponible pour les tâches de contrôle en mode d'affichage de la fenêtre agrandi et réduit.

Remarque
En cas de tâche de contrôle, dans la fenêtre de dialogue Sélection du profil, il est possible de sélectionner aussi bien des profils standard prédéfinis que des

profils personnalisés. Le profil Sélection manuelle est toujours exécuté avec la sélection actuelle.

7.3.12 Rapports

La rubrique **Rapports** permet d'afficher les résultats des actions effectuées par le programme.

Barre d'outils, commande clavier et menu contextuel

Icône	Commande clavier	Description
	Entrée	**Afficher le rapport** Ouvre une fenêtre dans laquelle le résultat de l'action sélectionnée s'affiche. Par exemple, le résultat d'une recherche.
	F3	**Afficher le fichier rapport** Affiche le fichier rapport correspondant au rapport sélectionné.
	F4	**Imprimer le fichier rapport** Ouvre la boîte de dialogue Windows Imprimer pour l'impression du fichier rapport.
	Suppr	**Supprimer le(s) rapport(s)** Supprime le rapport sélectionné et le fichier rapport correspondant.

Tableau

État

Icône	Description
✅	Action recherche : aucun résultat positif
⚠	Action recherche : virus détecté ou a échoué
(icône verte)	Action mise à jour : mise à jour réussie
(icône rouge)	Action mise à jour : échec de la mise à jour

Action

Indique l'action entreprise.

Résultat

Indique le résultat de l'action.

Date/Heure

Indique la date et l'heure à laquelle le rapport a été généré.

Contenu d'un rapport pour une recherche

- *Date de la recherche :*

  Date de la recherche.
- *Heure de début de la recherche :*

  Heure de début de la recherche.
- *Temps de recherche nécessaire :*

  Indique le temps au format mm:ss.
- *État de contrôle :*

  Indique si la tâche de contrôle a été effectuée complètement ou si elle a été interrompue.
- *Dernier résultat positif :*

  Nom du dernier virus ou programme indésirable trouvé.
- *Répertoires contrôlés :*

  Nombre total des répertoires parcourus.
- *Fichiers contrôlés :*

  Nombre total de fichiers parcourus.
- *Archives contrôlées :*

Nombre d'archives parcourues.

- *Objets cachés :*

  Nombre total d'objets cachés détectés.
- *Trouvé :*

  Nombre total des virus et programmes indésirables découverts.
- *Suspect :*

  Nombre de fichiers suspects.
- *Avertissements :*

  Nombre de messages d'avertissement relatifs à des virus détectés.
- *Remarques :*

  Nombre de remarques publiées, par ex. les informations complémentaires qui peuvent apparaître pendant une recherche.
- *Réparé :*

  Nombre total des fichiers réparés.
- *Quarantaine :*

  Nombre total des fichiers déplacés en quarantaine.
- *Renommé :*

  Nombre total des fichiers renommés.
- *Supprimé :*

  Nombre total des fichiers supprimés.
- *Écrasé :*

  Nombre total des fichiers écrasés.

Remarque
Les rootkits ont la propriété de dissimuler des processus et objets comme les entrées de registres ou les fichiers, toutefois chaque objet dissimulé ne prouve pas nécessairement l'existence d'un rootkit. En cas d'objets cachés, il peut également s'agir d'objets inoffensifs. Lors de la recherche, si des objets cachés sont trouvés et s'il n'y a aucun message d'avertissement relatif à des virus détectés, vous devez indiquer, à l'aide du rapport, de quels objets il s'agit et demander d'autres informations sur les objets trouvés.

7.3.13 Événements

La rubrique **Événements** indique les événements générés par les différents composants du programme.

Les événements sont enregistrés dans une base de données. Vous pouvez activer ou désactiver la limitation de la taille de la base de données d'événements (voir Événements). Par défaut, seuls les événements des 30 derniers jours sont enregistrés. L'affichage des événements est automatiquement actualisé lorsque vous sélectionnez la rubrique **Événements**.

> **Remarque**
> L'affichage des événements n'est pas actualisé automatiquement si la base de données contient plus de 20 000 événements. Dans ce cas, appuyez sur F5 pour actualiser l'affichage des événements.

Barre d'outils, commande clavier et menu contextuel

Icône	Commande clavier	Description
i	Entrée	**Afficher l'événement sélectionné** Ouvre une fenêtre dans laquelle l'événement d'une action sélectionnée s'affiche. Par exemple le résultat d'une recherche.
	F3	**Exporter le ou les événement(s) sélectionné(s)** Exporte les événements sélectionnés.
×	Suppr	**Supprimer le ou les événement(s) sélectionné(s)** Supprime un événement sélectionné.

> **Remarque**
> Vous pouvez exécuter des actions pour plusieurs événements sélectionnés. Pour sélectionner plusieurs événements, maintenez la touche Ctrl ou Maj (sélection d'événements situés les uns sous les autres) enfoncée pendant la sélection des éléments. Pour sélectionner tous les événements affichés, appuyez sur Ctrl + A.
> L'action Afficher l'événement sélectionné ne peut pas être exécutée sur une sélection d'objet multiple.

Modules

Les événements des modules suivants (présentés ici par ordre alphabétique) peuvent être visualisés à l'aide de l'affichage des événements :

Désignation du module
Protection Web
Protection temps réel
Protection e-mail
Service d'assistance
Planificateur
Scanner
Updater

En activant la case à cocher **Tous**, vous pouvez afficher les événements de tous les modules disponibles. Pour visionner uniquement les événements d'un module défini, cochez la case en regard du module souhaité.

Filtre

Dans l'affichage des événements, ces types d'événements s'affichent :

Icône	Description
	Information
	Avertissement
	Erreur
	Résultat positif

En activant la case à cocher **Filtre**, vous pouvez afficher tous les événements. Pour n'afficher que certains événements, cochez la case en regard de l'événement souhaité.

Tableau

L'affichage des événements contient les informations suivantes :

Icône

Icône d'affichage du type d'événement.

Type

Classification de l'événement : information, avertissement, erreur, résultat positif.

Module

Module Avira qui a enregistré cet événement. Par exemple, la protection temps réel qui a constaté un résultat positif.

Action

Description d'événement du module en question.

Date/Heure

Date et heure locale de l'événement.

7.3.14 Actualiser

Met à jour l'affichage de la rubrique ouverte.

7.4 Extras

7.4.1 Scanner les secteurs d'amorçage

Vous pouvez aussi scanner les secteurs d'amorçage des lecteurs de votre poste de travail par une recherche directe. Cette action est recommandée si un virus a été détecté lors d'une recherche directe et si vous souhaitez vous assurer que les secteurs d'amorçage ne sont pas affectés.

Il est possible de sélectionner plusieurs secteurs d'amorçage en maintenant la touche Maj (touche majuscule) enfoncée pendant que vous sélectionnez les lecteurs avec la souris.

> **Remarque**
> Vous pouvez faire scanner automatiquement les secteurs d'amorçage à chaque recherche directe (voir Secteur d'amorçage Lecteurs recherche).

> **Remarque**
> Sous Windows Vista, le contrôle des secteurs d'amorçage n'est possible qu'avec les droits d'administrateur.

7.4.2 Liste des menaces détectées

Cette fonction répertorie les noms des virus et programmes indésirables pouvant être détectés par votre produit Avira. Une fonction pratique de recherche des noms est intégrée.

Chercher dans la liste des menaces détectées

Dans le champ *Rechercher*, entrez un terme de recherche ou une suite de caractères.

Rechercher une suite de caractères dans un nom

Vous pouvez entrer ici une suite de lettres ou de caractères via le clavier, le repère passe au premier emplacement de la liste des noms où cette suite de caractères se trouve - même au milieu d'un nom (exemple : vous pouvez trouver « Abraxas » en tapant « raxa »).

Rechercher à partir du premier caractère d'un nom

Vous pouvez saisir ici l'initiale et les caractères suivants sur le clavier, le repère contrôle la liste des noms dans l'ordre alphabétique (exemple : vous pouvez trouver « Rabbit » en tapant « Ra »).

Si le nom ou la suite de caractères se trouve dans la liste, son emplacement y est repéré.

Chercher en avant

Démarre la recherche vers l'avant, dans l'ordre alphabétique.

Chercher en arrière

Démarre la recherche vers l'arrière, dans l'ordre alphabétique.

Premier résultat positif

Repasse à la première entrée précédente trouvée dans la liste.

Entrées dans la liste des menaces détectées

Cet intitulé recouvre une liste de noms des virus ou programmes indésirables qui peuvent être détectés. La plupart des entrées de cette liste peuvent également être supprimées à l'aide de votre produit Avira. Elles sont dans l'ordre alphabétique (d'abord les caractères spéciaux et les chiffres, puis les lettres). Utilisez la barre de défilement pour monter ou descendre dans la liste.

7.4.3 Télécharger le CD de secours

La commande de menu **Télécharger le CD de secours** vous permet de lancer le téléchargement du pack du CD de secours Avira. Le pack contient un système live de démarrage pour PC ainsi qu'un scanner antivirus Avira avec un fichier de définitions des virus et un moteur de recherche mis à jour. Vous utilisez le CD de secours Avira pour

démarrer et utiliser votre PC à partir du CD ou DVD si votre système d'exploitation est endommagé, afin de récupérer des données ou d'effectuer une recherche de virus et de logiciels malveillants.

Une fois le pack du CD de secours Avira téléchargé, une fenêtre de dialogue s'affiche dans laquelle vous sélectionnez un lecteur CD/DVD en vue de graver le CD de secours. Vous pouvez également enregistrer le pack du CD de secours Avira, afin de graver le CD de secours à une date ultérieure.

> **Remarque**
> Vous avez besoin d'une connexion Internet active pour télécharger le pack du CD de secours Avira. Vous avez besoin d'un lecteur CD/DVD et d'un CD ou DVD inscriptible pour graver le CD de secours.

7.4.4 Configuration

La rubrique **Configuration** du menu **Extras** ouvre la Configuration.

7.5 Mise à jour

7.5.1 Démarrer mise à jour...

La rubrique **Démarrer mise à jour...** du menu **Mise à jour** lance une mise à jour immédiate. Le fichier de définitions des virus et le moteur de recherche sont mis à jour.

7.5.2 Mise à jour manuelle...

La rubrique **Mise à jour manuelle...** du menu **Mise à jour** ouvre une fenêtre de dialogue permettant de sélectionner et de charger un pack de mise à jour du moteur/VDF. Le pack de mise à jour peut être téléchargé depuis le site Web du fabricant et contient le fichier de définitions des virus et le moteur de recherche actuels :
http://www.avira.com/fr

> **Remarque**
> Sous Windows Vista, une mise à jour manuelle n'est possible qu'avec les droits d'administrateur.

7.6 Aide

7.6.1 Sujets

La rubrique **Sujets** du menu **Aide** ouvre le sujets de l'aide en ligne.

7.6.2 Aidez-moi

Si une connexion Internet est active, la rubrique **Aidez-moi** du menu **Aide** ouvre la page de support correspondant à votre produit sur le site Web d'Avira. Vous pouvez y lire les réponses aux questions fréquemment posées, accéder à la base de connaissances ou contacter le service clientèle d'Avira.

7.6.3 Aide en ligne

Si une connexion Internet est active, la commande **Aide en ligne** du menu **Aide** ouvre le site Web d'Avira. Téléchargez l'outil Module client de support d'Avira. Le module client permet la connexion à distance avec le support d'Avira. Après avoir téléchargé et installé le module, contactez le support d'Avira par téléphone afin de communiquer l'ID de votre module et convenir d'une date de maintenance à distance.

7.6.4 Forum

Si une connexion Internet est active, la rubrique **Forum** du menu **Aide** ouvre une page Web vous permettant d'accéder au forum d'Avira.

7.6.5 Télécharger le manuel

Si une connexion Internet est active, la rubrique **Télécharger le manuel** du menu **Aide** ouvre une page de téléchargement de votre produit Avira. Vous trouverez sur cette page un lien permettant de télécharger le manuel le plus récent pour votre produit Avira.

7.6.6 Gestion des licences

La rubrique **Gestion des licences** du menu **Aide** ouvre l'assistant de licence. Cet assistant vous aide à acquérir une licence ou activer votre produit Avira simplement.

Activer le produit

Activez cette option si vous disposez déjà d'un code d'activation et que le produit Avira n'est pas encore activé. Lors de l'activation du produit, vous êtes inscrit en tant que client et le produit Avira est activé avec votre licence. Soit nous vous avons envoyé le code d'activation par e-mail, soit celui-ci est indiqué sur l'emballage du produit.

> **Remarque**
> Le programme peut être réactivé avec un code d'activation valide si cela est nécessaire en raison d'une réinstallation du système.

> **Remarque**
> Pour activer le produit, le programme communique avec les serveurs d'Avira via le protocole HTTP et le port 80 (communication Web) ainsi que via le protocole de cryptage SSL et le port 443. Si vous utilisez un pare-feu, assurez-vous que celui-ci ne bloque pas les connexions nécessaires ni les données entrantes ou sortantes.

> **Remarque**
> Vous pouvez lancer une mise à niveau pour un produit de la gamme Avira Desktop (voir Attribution de licence et mise à niveau). Dans le champ Code d'activation, entrez le code d'activation du produit auquel vous souhaitez passer. Si une mise à niveau est possible, le produit s'installe automatiquement.

Acheter/Prolonger la licence

Cette option s'affiche si votre licence a expiré, si elle est encore valable ou si vous ne disposez que d'une licence d'évaluation. Utilisez cette option pour prolonger la licence de votre produit ou acheter une licence complète. Pour ce faire, vous avez besoin d'une connexion Internet active : sélectionnez l'option *Acheter/Prolonger la licence* et cliquez sur **Suivant**. Votre navigateur Internet s'ouvre à la page de la boutique en ligne d'Avira, où vous avez la possibilité d'acquérir une licence.

Fichier de licence valide

Vous pouvez lire un fichier de licence valide via le lien **Fichier de licence**.
Le fichier de licence est généré avec un code d'activation valide lors du processus d'activation du produit ; il est enregistré dans le répertoire de votre produit Avira et lu. N'utilisez cette option qu'après avoir activé votre produit.

Paramètres de proxy...

Si vous cliquez sur ce bouton, une fenêtre de dialogue s'ouvre. Si nécessaire, vous pouvez paramétrer la connexion Internet utilisée pour l'activation du produit pour y accéder via un serveur proxy.

7.6.7 Recommander le produit

Si une connexion Internet est active, la commande **Recommander un produit** du menu **Aide** ouvre un site Web destiné aux clients d'Avira. Vous pouvez y recommander votre produit Avira et bénéficier ainsi des offres promotionnelles d'Avira.

7.6.8 Envoyer un commentaire

Si une connexion Internet est active, la commande **Envoyer un commentaire** du menu **Aide** ouvre une page de commentaires concernant les produits Avira. Vous y trouverez un formulaire d'évaluation de produit que vous pouvez envoyer à Avira avec votre avis quant à la qualité du produit et d'autres remarques concernant le produit.

7.6.9 À propos de Avira Antivirus Suite

Généralités

Adresses et informations sur votre produit Avira

Informations de version

Informations sur la version des fichiers se trouvant dans le pack produit Avira

Informations de licence

Informations sur la licence actuelle et liens vers la boutique en ligne (achat ou prolongation d'une licence)

> **Remarque**
> Vous pouvez enregistrer les données de licence dans la mémoire tampon. Cliquez sur la zone Données de licence avec le bouton droit de la souris. Un menu contextuel s'ouvre. Dans le menu contextuel, cliquez sur la commande **Copier dans la mémoire tampon**. Vos données de licence sont maintenant enregistrées dans la mémoire tampon et peuvent être ajoutées dans des e-mails, des formulaires ou des documents via la commande Windows correspondante.

8. Protection mobile

Avira ne protège pas uniquement votre ordinateur des virus et logiciels malveillants, mais empêche également la perte et/ou le vol des téléphones portables et smartphones équipés d'un système d'exploitation Android. La liste noire d'Avira Free Android Security vous permet en outre de bloquer les appels et SMS indésirables. Il vous suffit d'ajouter des numéros de téléphone à la liste noire depuis votre journal d'appels, votre journal de SMS ou votre liste de contacts, ou de créer manuellement des contacts que vous souhaitez bloquer.

Vous trouverez de plus amples informations sur notre site Web :

www.avira.com/android

9. Configuration

9.1 Configuration

- Aperçu des options de configuration
- Boutons

9.1.1 Aperçu des options de configuration

Vous disposez des options de configuration suivantes :

- **Scanner** : configuration de la recherche directe
  - Options de recherche
  - Action si résultat positif
  - Options pour la recherche dans les archives
  - Exceptions de la recherche directe
  - Heuristique de la recherche directe
  - Réglage de la fonction de rapport
- **Protection temps réel** : configuration de la recherche en temps réel
  - Options de recherche
  - Action si résultat positif
  - Exceptions de la recherche en temps réel
  - Heuristique de la recherche en temps réel
  - Réglage de la fonction de rapport
- **Mise à jour** : configurations des paramètres de mise à jour
  - Télécharger via le serveur Web
  - Paramètres proxy
- **Protection Web** : configuration de la protection Web
  - Options de recherche, activation et désactivation de la protection Web
  - Action si résultat positif
  - Accès bloqués : types de fichiers et types MIME indésirables, filtre Web pour les URL connues indésirables (logiciels malveillants, hameçonnage, etc.)
  - Exceptions de recherche de la protection Web : URL, types de fichiers, types MIME
  - Heuristique de la protection Web
  - Réglage de la fonction de rapport
- **Protection e-mail** : configuration de la protection e-mail
  - Options de recherche : activation de la surveillance des comptes POP3, des comptes IMAP, des e-mails sortants (SMTP)



- Action si résultat positif
- Autres actions
- Heuristique de la recherche de la protection e-mail
- Fonction AntiBot : serveurs SMTP autorisés, expéditeurs d'e-mails autorisés
- Exceptions de la recherche de la protection e-mail
- Configuration de la mémoire tampon, vider la mémoire tampon
- Réglage de la fonction de rapport

- **Généralités** :
  - Catégories étendues de dangers pour la recherche directe et en temps réel
  - Protection étendue : options pour activer ProActiv et la protection Cloud
  - Filtre des applications : bloquer ou autoriser des applications
  - Protection par mot de passe pour l'accès au Control Center et à la configuration
  - Sécurité : bloquer les fonctions Autorun, verrouiller les fichiers hôtes Windows, protection du produit
  - WMI : activer la prise en charge WMI
  - Configuration de la consignation des événements
  - Configuration des fonctions de rapport
  - Réglage des répertoires utilisés
  - Configuration des avertissements sonores en cas de détection de logiciel malveillant

Boutons

Bouton	Description
Valeurs par défaut	Tous les paramètres de la configuration sont réinitialisés aux valeurs par défaut. Toutes les modifications et vos saisies sont perdues en cas de restauration des valeurs par défaut.
OK	Tous les paramètres définis sont enregistrés. La configuration se referme. Le contrôle de compte d'utilisateur (UAC) a besoin de votre accord pour appliquer les modifications apportées dans les systèmes d'exploitation à partir de Windows Vista.

Annuler	La configuration se referme sans que les paramètres que vous avez définis ne soient enregistrés dans la configuration.
Appliquer	Tous les paramètres définis sont enregistrés. Le contrôle de compte d'utilisateur (UAC) a besoin de votre accord pour appliquer les modifications apportées dans les systèmes d'exploitation à partir de Windows Vista.

9.2 Scanner

La rubrique **Scanner** de la configuration est en charge de la configuration de la recherche directe, c'est-à-dire de la recherche à la demande.

9.2.1 Recherche

Vous pouvez définir le comportement de base de la routine de recherche lors d'une recherche directe. Si vous choisissez certains répertoires à contrôler lors de la recherche directe, le scanner effectue le contrôle en fonction de la configuration :

- avec un niveau de recherche défini (priorité),
- plus les secteurs d'amorçage et la mémoire principale,
- tous les fichiers du répertoire, ou seulement certains.

Fichiers

Le scanner peut utiliser un filtre pour ne contrôler que les fichiers avec une extension particulière (type).

Tous les fichiers

Si cette option est activée, tous les fichiers sont parcourus à la recherche de virus et programmes indésirables, quels que soient leur contenu et leur extension. Le filtre n'est pas utilisé.

> **Remarque**
> Si l'option **Tous les fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Sélection intelligente des fichiers

Si cette option est activée, la sélection des fichiers à contrôler est effectuée automatiquement par le programme. Cela signifie que votre programme Avira décide en fonction du contenu d'un fichier si celui-ci doit être contrôlé quant à l'absence de

virus et programmes indésirables. Ce processus est un peu plus lent que l'option **Utiliser la liste des extensions de fichiers**, mais beaucoup plus sûr, car le contrôle n'a pas lieu uniquement sur la base des extensions de fichiers. Ce paramètre est activé par défaut et recommandé.

> **Remarque**
> Si l'option **Sélection intelligente des fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Utiliser la liste des extensions de fichiers

Si cette option est activée, seuls les fichiers dont l'extension a été présélectionnée sont contrôlés. Sont présélectionnés par défaut tous les types de fichiers pouvant contenir des virus et programmes indésirables. Cette liste peut être modifiée manuellement à l'aide du bouton « **Extensions de fichiers** ».

> **Remarque**
> Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci est signalé avec le texte « *Aucune extension de fichiers* », sous le bouton **Extensions de fichiers**.

Extensions de fichiers

Ce bouton permet d'ouvrir une boîte de dialogue contenant toutes les extensions de fichiers examinées lors d'une recherche en mode « **Utiliser la liste des extensions de fichiers** ». Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

> **Remarque**
> Notez que la liste par défaut peut changer d'une version à l'autre.

Autres paramètres

Secteur d'amorçage des lecteurs

Si cette option est activée, le scanner contrôle les secteurs d'amorçage des lecteurs sélectionnés pour la recherche directe. Ce paramètre est activé par défaut.

Scanner les secteurs d'amorçage maître

Si cette option est activée, le scanner contrôle les secteurs d'amorçage maître du ou des disques durs utilisés dans le système.

Ignorer les fichiers hors ligne

Si cette option est activée, la recherche directe ignore complètement les fichiers hors ligne lors d'une recherche. Cela signifie que la présence de virus et programmes

indésirables n'est pas contrôlée sur ces fichiers. Les fichiers hors ligne sont des fichiers qui ont été déplacés physiquement par un système de gestion hiérarchique de la mémoire (HSMS), du disque dur vers une bande, par exemple. Ce paramètre est activé par défaut.

Contrôle d'intégrité de fichiers système

Si cette option est activée, les fichiers système Windows les plus importants sont soumis à un contrôle particulièrement sûr concernant d'éventuelles modifications opérées par des logiciels malveillants, et ce à chaque recherche directe. Si un fichier modifié est trouvé, celui-ci est signalé comme résultat positif suspect. Cette fonction utilise beaucoup de ressources de l'ordinateur. C'est pourquoi l'option est désactivée par défaut.

Remarque
Cette fonction n'est disponible qu'à partir de Windows Vista.

Remarque
Si vous utilisez des outils de fournisseurs tiers qui modifient les fichiers système et adaptent l'écran d'amorçage ou de démarrage à vos besoins, veuillez ne pas utiliser cette option. Voici quelques exemples de ces outils : Skinpacks, TuneUp Utilities ou Vista Customization.

Recherche optimisée

Si cette option est activée, la capacité du processeur est utilisée de façon optimale lors d'une recherche effectuée par le scanner. Pour des raisons liées à la performance, la consignation lors d'une recherche optimisée s'effectue au maximum à un niveau par défaut.

Remarque
L'option n'est disponible que sur les ordinateurs multiprocesseurs.

Suivre les liens symboliques

Si cette option est activée, le scanner suit, lors d'une recherche, tous les liens symboliques du profil de recherche ou du répertoire sélectionné pour contrôler l'absence de virus et de logiciels malveillants dans les fichiers liés.

Remarque
L'option n'inclut aucun lien de fichiers (shortcuts) mais se réfère exclusivement aux liens symboliques (créés avec mklink.exe) ou aux Junction Points (créés

avec junction.exe) qui sont présents de manière transparente dans le système de fichiers.

Recherche de rootkits en début de contrôle

Si cette option est activée, le scanner vérifie au démarrage le répertoire système Windows à la recherche de rootkits actifs, au moyen d'un processus dit accéléré. Ce processus contrôle l'absence de rootkits sur votre ordinateur de manière moins détaillée que le profil de recherche « **Recherche de rootkits** », il est toutefois exécuté beaucoup plus rapidement. Cette option ne modifie que les paramètres des profils que vous avez personnellement créés.

Remarque
La recherche de rootkits n'est pas disponible sous Windows XP 64 bits .

Scanner le Registre

Si cette option est activée, le système recherche la présence de renvois à des logiciels dommageables dans le Registre. Cette option ne modifie que les paramètres des profils que vous avez personnellement créés.

Ignorer les fichiers et les chemins sur les lecteurs réseau

Si cette option est activée, les lecteurs réseau reliés à l'ordinateur sont exclus de la recherche directe. Cette option est recommandée quand les serveurs ou d'autres postes de travail sont eux-mêmes protégés par un logiciel antivirus. Cette option est désactivée par défaut.

Processus de contrôle

Autoriser l'arrêt

Si cette option est activée, la recherche de virus ou programmes indésirables peut être arrêtée à tout moment avec le bouton « **Arrêt** » dans la fenêtre « **Luke Filewalker** ». Si vous avez désactivé ce paramètre, le bouton **Arrêt** est grisé dans la fenêtre « **Luke Filewalker** ». L'arrêt prématurée d'une recherche n'est alors pas possible. Ce paramètre est activé par défaut.

Priorité du scanner

Le scanner distingue trois niveaux de priorité lors de la recherche directe. Cette distinction ne s'applique que si plusieurs processus fonctionnent en même temps sur l'ordinateur. Le choix influe sur la vitesse de la recherche.

Basse

Le scanner reçoit du système d'exploitation du temps processeur uniquement si aucun autre processus ne nécessite de temps de calcul, c'est-à-dire que tant que le scanner fonctionne seul, la vitesse est maximale. Globalement, le travail avec les autres

programmes est ainsi facilité : l'ordinateur réagit plus vite si d'autres programmes ont besoin de temps de calcul, pendant que le scanner continue de tourner en arrière-plan.

Moyenne

Le scanner est exécuté avec le niveau de priorité normal. Tous les processus reçoivent du système d'exploitation le même temps processeur. Ce paramètre est activé par défaut et recommandé. Dans certaines conditions, le travail avec d'autres applications peut être entravé.

Élevée

Le scanner obtient la priorité la plus élevée. Le travail en parallèle avec d'autres applications n'est quasiment plus possible. Toutefois, le scanner effectue sa recherche à la vitesse maximale.

Action si résultat positif

Vous pouvez définir les actions que le scanner doit exécuter quand un virus ou programme indésirable a été détecté.

Interactif

Si l'option est activée, les résultats positifs de la recherche du scanner sont signalés dans une fenêtre de dialogue. Lors de la recherche du scanner, vous recevez à l'issue de la recherche un message d'avertissement comportant une liste des fichiers contaminés qui ont été trouvés. Vous avez la possibilité de sélectionner une action à exécuter pour les différents fichiers concernés, via le menu contextuel. Vous pouvez exécuter les actions choisies pour tous les fichiers concernés ou quitter le scanner.

> **Remarque**
> L'action **Quarantaine** est présélectionnée par défaut dans la boîte de dialogue pour le traitement des virus. Vous pouvez sélectionner d'autres actions via un menu contextuel.

Automatique

Si l'option est activée, aucune boîte de dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. Le scanner réagit en fonction des paramètres que vous avez définis dans cette section.

Copier le fichier en quarantaine avant l'action

Si l'option est activée, le scanner génère une copie de sauvegarde (backup) avant d'exécuter l'action primaire ou secondaire souhaitée. La copie de sauvegarde est conservée en quarantaine où le fichier peut être restauré s'il a une valeur informative. En outre, vous pouvez envoyer la copie de sauvegarde à l'Avira Malware Research Center pour d'autres analyses.

Action primaire

L'action primaire est l'action exécutée lorsque le scanner trouve un virus ou un programme indésirable. Si l'option « **Réparer** » est sélectionnée, mais que la réparation du fichier contaminé est impossible, l'action sélectionnée sous « **Action secondaire** » est exécutée.

Remarque
L'option **Action secondaire** ne peut être sélectionnée que si, sous **Action primaire**, le paramètre **Réparer** a été sélectionné.

Réparer

Si l'option est activée, le scanner répare automatiquement les fichiers contaminés. Si le scanner ne peut pas réparer un fichier contaminé, il exécute comme solution de rechange l'option choisie sous Action secondaire.

Remarque
Une réparation automatique est recommandée, mais cela signifie que le scanner modifie les fichiers sur l'ordinateur.

Renommer

Si l'option est activée, le scanner renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, le scanner déplace le fichier en quarantaine. Ces fichiers peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus **Écraser et supprimer** (voir ci-dessous).

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, le scanner remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Action secondaire

L'option « **Action secondaire »** ne peut être sélectionnée que si le paramètre **Réparer** a été sélectionnée sous « **Action primaire »**. Cette option permet de décider ce qui doit advenir du fichier contaminé s'il n'est pas réparable.

Renommer

Si l'option est activée, le scanner renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, le scanner déplace le fichier en quarantaine. Ces fichiers peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus d'écrasement et de suppression.

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, le scanner remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Remarque
Si vous avez sélectionné **Supprimer** ou **Écraser et supprimer** comme action primaire ou secondaire, tenez compte de ce qui suit : dans le cas de résultats heuristiques, les fichiers contaminés ne sont pas supprimés, mais déplacés en quarantaine.

Archives

Lors de la recherche dans les archives, le scanner peut utiliser une recherche récursive : les archives dans les archives sont décompressées et l'absence de virus et de programmes indésirables est contrôlée. Les fichiers sont contrôlés, décompressés et à nouveau contrôlés.

Contrôler les archives

Si cette option est activée, les archives sélectionnées dans la liste des archives sont contrôlées. Ce paramètre est activé par défaut.

Tous les types d'archives

Si cette option est activée, toutes les archives figurant dans la liste des archives sont sélectionnées et contrôlées.

Extensions intelligentes

Si cette option est activée, le scanner détecte si un fichier présente un format compressé (archive), même quand l'extension diffère des extensions habituelles, et contrôle l'archive. Pour cela, chaque fichier doit être ouvert, ce qui réduit la vitesse de recherche. Exemple : si une archive *.zip est dotée de l'extension *.xyz, le scanner décompresse également cette archive et la contrôle. Ce paramètre est activé par défaut.

> **Remarque**
> Seuls les types d'archives sélectionnés dans la liste des archives sont contrôlés.

Limiter la profondeur de récursivité

La décompression et le contrôle des archives à imbrication très profonde peut nécessiter beaucoup de temps de calcul et de ressources. Si cette option est activée, la profondeur de la recherche est limitée dans les archives multicompressées à un nombre défini sur les niveaux de paquets (profondeur de récursivité maximale). Vous économisez ainsi du temps et des ressources.

> **Remarque**
> Pour déterminer s'il y a un virus ou un programme indésirable au sein d'une archive, le scanner doit scanner celle-ci jusqu'au niveau de récursivité dans lequel le virus ou le programme indésirable se trouve.

Profondeur maximale de récursivité

Pour pouvoir saisir la profondeur de récursivité maximale, l'option **Limiter la profondeur de récursivité** doit être activée.
Vous pouvez soit saisir directement la profondeur de récursivité souhaitée, soit la modifier avec les touches fléchées à droite du champ de saisie. Les valeurs autorisées vont de 1 à 99. La valeur par défaut recommandée est de 20.

Valeurs par défaut

Le bouton restaure les valeurs prédéfinies pour la recherche dans les archives.

Liste des archives

Dans cette zone d'affichage, vous pouvez définir quelles archives le scanner doit contrôler. Pour cela, vous devez sélectionner les entrées correspondantes.

Exceptions

Objets de fichier à exclure par le scanner

La liste dans cette fenêtre contient les fichiers et chemins que le scanner doit ignorer lors de la recherche de virus et programmes indésirables.

Entrez ici aussi peu d'exceptions que possible et uniquement les fichiers qui ne doivent vraiment pas être contrôlés lors d'une recherche normale, pour quelque motif que ce soit. Nous recommandons dans tous les cas de contrôler l'absence de virus et de programmes indésirables sur ces fichiers, avant de les mettre dans la liste.

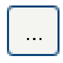
Remarque
Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Avertissement
Ces fichiers sont ignorés lors de la recherche.

Remarque
Les fichiers inscrits dans cette liste sont mentionnés dans le fichier rapport. Contrôlez de temps en temps le fichier rapport concernant ces fichiers non contrôlés car la raison pour laquelle vous aviez exclu un fichier n'existe peut-être plus. Dans ce cas, supprimez le nom de ce fichier de la liste.

Champ de saisie

Entrez dans ce champ le nom de l'objet de fichier qui doit être ignoré par la recherche directe. Aucun objet de fichier n'est indiqué par défaut.



Ce bouton ouvre une fenêtre dans laquelle vous pouvez sélectionner le fichier ou le chemin souhaité.
Si vous avez saisi un nom de fichier avec le chemin intégral, seul ce fichier n'est pas contrôlé. Si vous avez saisi un nom de fichier sans chemin, tout fichier portant ce nom (quel que soit le chemin ou le lecteur) ne sera pas contrôlé.

Ajouter

Ce bouton vous permet de reprendre dans la fenêtre d'affichage l'objet de fichier entré dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche.

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre programme Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

9.2.2 Rapport

Le scanner dispose d'une fonction de consignation étendue. Vous obtenez ainsi des informations précises sur les résultats d'une recherche directe. Le fichier rapport contient toutes les données du système, ainsi que les avertissements et messages de la recherche directe.

> **Remarque**
> Pour vous permettre de savoir quelles actions le scanner a effectuées lors de la détection de virus ou de programmes indésirables, un fichier rapport doit systématiquement être généré.

Consignation

Désactivée

Si cette option est activée, le scanner ne consigne pas les actions et résultats de la recherche directe.

Par défaut

Si cette option est activée, le scanner consigne les noms des fichiers contaminés en indiquant leur chemin. En outre, la configuration de la recherche actuelle, les informations sur la version et sur le détenteur de la licence sont inscrites dans le fichier rapport.

Étendue

Si cette option est activée, le scanner consigne les avertissements et remarques en plus des informations standard. Le fichier rapport mentionne un suffixe « (Cloud) » pour identifier les avertissements de la protection Cloud.

Intégrale

Si cette option est activée, le scanner consigne également tous les fichiers contrôlés. En outre, tous les fichiers contaminés, ainsi que les avertissements et remarques sont repris dans le fichier rapport.

> **Remarque**
> Si vous devez nous envoyer un fichier rapport (pour la recherche d'erreur), merci de le générer dans ce mode.

9.3 Protection temps réel

La rubrique Protection temps réel de la configuration permet la configuration de la recherche en temps réel.

9.3.1 Recherche

En règle générale, vous voudrez surveiller votre système en continu. Pour ce faire, utilisez la protection temps réel (recherche en temps réel = On-Access Scanner). Cette protection vous permet de faire contrôler « à la volée » tous les fichiers copiés ou ouverts sur l'ordinateur à la recherche de virus et de programmes indésirables.

Fichiers

La protection temps réel peut utiliser un filtre pour ne contrôler que les fichiers avec une certaine extension (type).

Tous les fichiers

Si cette option est activée, tous les fichiers sont parcourus à la recherche de virus et programmes indésirables, quels que soient leur contenu et leur extension.

> **Remarque**
> Si l'option **Tous les fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Sélection intelligente des fichiers

Si cette option est activée, la sélection des fichiers à contrôler est effectuée automatiquement par le programme. Cela signifie que le programme décide en fonction du contenu d'un fichier si celui-ci doit être contrôlé quant à l'absence de virus et programmes indésirables. Ce processus est un peu plus lent que l'option **Utiliser la liste des extensions de fichiers**, mais beaucoup plus sûr, car le contrôle n'a pas lieu uniquement sur la base des extensions de fichiers.

> **Remarque**
> Si l'option **Sélection intelligente des fichiers** est activée, le bouton **Extensions de fichiers** ne peut pas être utilisé.

Utiliser la liste des extensions de fichiers

Si cette option est activée, seuls les fichiers dont l'extension a été présélectionnée sont contrôlés. Sont présélectionnés par défaut tous les types de fichiers pouvant contenir des virus et programmes indésirables. Cette liste peut être modifiée manuellement à l'aide du bouton « **Extension de fichiers** ». Ce paramètre est activé par défaut et recommandé.

> **Remarque**
> Si cette option est activée et que vous avez supprimé toutes les entrées de la liste des extensions de fichiers, ceci est signalé avec le texte « *Aucune extension de fichiers* », sous le bouton **Extensions de fichiers**.

Extensions de fichiers

Ce bouton permet d'ouvrir une boîte de dialogue contenant toutes les extensions de fichiers examinées lors d'une recherche en mode « **Utiliser la liste des extensions de fichiers** ». Pour les extensions, des entrées sont indiquées par défaut, mais il est possible d'ajouter et de supprimer des entrées.

Remarque
Notez que la liste des extensions de fichiers peut changer d'une version à l'autre.

Lecteurs

Surveiller les lecteurs réseau

Si cette option est activée, les fichiers se trouvant sur les lecteurs réseau (lecteurs mappés), comme les volumes de serveur, les lecteurs clients, etc., sont surveillés.

Remarque
Pour ne pas trop restreindre les performances de votre ordinateur, activez l'option **Surveiller les lecteurs réseau** uniquement dans des cas exceptionnels.

Avertissement
Si l'option est désactivée, les lecteurs réseau ne sont **pas** surveillés. Vous n'êtes plus protégé des virus et programmes indésirables.

Remarque
Quand des fichiers sont exécutés sur des lecteurs réseau, ceux-ci sont contrôlés par la protection temps réel, indépendamment du réglage de l'option **Surveiller les lecteurs réseau**. Dans certains cas, les fichiers se trouvant sur des lecteurs réseau sont contrôlés à leur ouverture, bien que l'option **Surveiller les lecteurs réseau** soit désactivée. La raison : l'accès à ces fichiers s'effectue avec le droit « Exécuter le fichier ». Si vous souhaitez exclure ces fichiers, ou bien aussi des fichiers exécutés sur les lecteurs réseau, de la surveillance opérée par la protection temps réel, veuillez inscrire les fichiers dans la liste des objets de fichiers à exclure (voir : Exceptions).

Activer la gestion d'antémémoire

Si cette option est activée, les fichiers surveillés sur les lecteurs réseau sont mis à disposition dans la gestion d'antémémoire de la protection temps réel. La surveillance des lecteurs réseau sans fonction de gestion d'antémémoire offre plus de sécurité mais est moins performante que la surveillance de lecteurs réseau avec la fonction de gestion d'antémémoire.

Archives

Contrôler les archives

Si l'option est activée, les archives sont contrôlées. Les fichiers compressés sont contrôlés, décompressés et à nouveau contrôlés. Cette option est désactivée par défaut. La recherche dans les archives est limitée par le biais de la profondeur de récursivité, du nombre de fichiers à analyser et de la taille des archives. Vous pouvez régler la profondeur maximale de récursivité, le nombre de fichiers à contrôler et la taille maximale des archives.

> **Remarque**
> Cette option est désactivée par défaut car le processus utilise beaucoup de ressources de l'ordinateur. Généralement, il est conseillé de contrôler les archives avec la recherche directe.

Prof. de récursivité max.

Lors de la recherche dans les archives, la protection temps réel peut utiliser une recherche récursive : les archives dans les archives sont décompressées et l'absence de virus et de programmes indésirables est contrôlée. Vous pouvez définir la profondeur de récursivité. La valeur par défaut pour la profondeur de récursivité, qui est de 1, est conseillée : tous les fichiers se trouvant directement dans l'archive principale sont contrôlés.

Nombre max. de fich.

Lors de la recherche dans les archives, celle-ci est limitée à un nombre maximal de fichiers dans l'archive. La valeur par défaut pour le nombre maximal de fichiers à contrôler est de 10 et est recommandée.

Taille max. (Ko)

Lors de la recherche dans les archives, celle-ci est limitée à une taille maximale d'archive à décompresser. La valeur par défaut de 1 000 Ko est recommandée.

Action si résultat positif

Vous pouvez établir des actions que la protection temps réel doit exécuter quand un virus ou programme indésirable a été détecté.

Interactif

Si l'option est activée, une notification est affichée sur le Bureau en cas de résultat positif de la protection temps réel. Vous avez la possibilité de supprimer le logiciel malveillant trouvé ou d'appeler d'autres actions possibles pour le traitement du virus via le bouton « **Détails** ». Les actions sont affichées dans une boîte de dialogue. Cette option est activée par défaut.

Réparer

La protection temps réel répare le fichier contaminé si c'est possible.



Renommer

La protection temps réel renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Le fichier peut être réparé ultérieurement et à nouveau renommé.

Quarantaine

La protection temps réel déplace le fichier en quarantaine. Le fichier peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center. Selon le fichier, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines (voir Gestionnaire de quarantaines).

Supprimer

Le fichier est supprimé. Cette opération est nettement plus rapide que le processus **Écraser et supprimer** (voir ci-dessous).

Ignorer

L'accès au fichier est autorisé et le fichier est conservé.

Écraser et supprimer

La protection temps réel remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Avertissement
Si la protection temps réel est réglée sur **Contrôler pendant l'écriture**, le fichier contaminé n'est pas créé.

Par défaut

Ce bouton vous permet de sélectionner l'action activée par défaut dans la boîte de dialogue en cas de détection d'un virus. Sélectionnez l'action qui doit être activée par défaut et cliquez sur le bouton **« Par défaut »**.

Remarque
L'action **Réparer** ne peut pas être sélectionnée comme action par défaut.

Vous trouverez de plus amples informations ici.

Automatique

Si l'option est activée, aucune boîte de dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. La protection temps réel réagit en fonction des paramètres que vous avez définis dans cette section.

Copier le fichier en quarantaine avant l'action

Si l'option est activée, la protection temps réel génère une copie de sauvegarde (backup) avant d'exécuter l'action primaire ou secondaire souhaitée. La copie de sauvegarde est conservée en quarantaine. Elle peut être restaurée à tout moment par le gestionnaire de quarantaines si elle a une valeur informative. En outre, vous pouvez envoyer la copie de sauvegarde à l'Avira Malware Research Center. En fonction de l'objet, d'autres possibilités de sélection sont disponibles dans le gestionnaire de quarantaines (voir Gestionnaire de quarantaines).

Action primaire

L'action primaire est l'action effectuée lorsque la protection temps réel trouve un virus ou un programme indésirable. Si l'option « **Réparer** » est sélectionnée, mais que la réparation du fichier contaminé est impossible, l'action sélectionnée sous « **Action secondaire** » est exécutée.

> **Remarque**
> L'option **Action secondaire** ne peut être sélectionnée que si, sous **Action primaire**, le paramètre **Réparer** a été sélectionné.

Réparer

Si l'option est activée, la protection temps réel répare automatiquement les fichiers contaminés. Si la protection temps réel ne peut pas réparer un fichier contaminé, elle exécute comme solution de rechange l'option choisie sous **Action secondaire**.

> **Remarque**
> Une réparation automatique est recommandée, mais cela signifie que la protection temps réel modifie les fichiers sur l'ordinateur.

Renommer

Si l'option est activée, la protection temps réel renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, la protection temps réel déplace le fichier dans un répertoire de quarantaine. Les fichiers de ce répertoire peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus d'écrasement et de suppression.

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

> **Avertissement**
> Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, la protection temps réel remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Refuser l'accès

Si l'option est activée, la protection temps réel inscrit le résultat positif dans le fichier rapport uniquement si la fonction de rapport est activée. En outre, la protection temps réel inscrit une entrée dans le protocole d'événements, si cette option est activée.

> **Avertissement**
> Si la protection temps réel est réglée sur **Contrôler pendant l'écriture**, le fichier contaminé n'est pas créé.

Action secondaire

L'option « **Action secondaire** » ne peut être sélectionnée que si l'option « **Réparer** » a été sélectionnée sous « **Action primaire** ». Cette option permet de décider ce qui doit advenir du fichier contaminé s'il n'est pas réparable.

Renommer

Si l'option est activée, la protection temps réel renomme le fichier. Un accès direct à ces fichiers (par un double clic par ex.) n'est alors plus possible. Les fichiers peuvent être réparés ultérieurement et à nouveau renommés.

Quarantaine

Si l'option est activée, la protection temps réel déplace le fichier en quarantaine. Les fichiers peuvent être réparés ultérieurement ou, si nécessaire, être envoyés à l'Avira Malware Research Center.

Supprimer

Si l'option est activée, le fichier est supprimé. Cette opération est nettement plus rapide que le processus d'écrasement et de suppression.

Ignorer

Si l'option est activée, l'accès au fichier est autorisé et le fichier est conservé.

> **Avertissement**
> Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Écraser et supprimer

Si l'option est activée, la protection temps réel remplace le fichier par un modèle par défaut et le supprime ensuite. Il ne peut plus être restauré.

Refuser l'accès

Si l'option est activée, le fichier contaminé n'est pas créé. La protection temps réel inscrit le résultat positif dans le fichier rapport uniquement si la fonction de rapport est activée. En outre, la protection temps réel inscrit une entrée dans le protocole d'événements, si cette option est activée.

> **Remarque**
> Si vous avez sélectionné **Supprimer** ou **Écraser et supprimer** comme action primaire ou secondaire, tenez compte de ce qui suit : dans le cas de résultats heuristiques, les fichiers contaminés ne sont pas supprimés, mais déplacés en quarantaine.

Autres actions

Utiliser le rapport d'événement

Si cette option est activée, une entrée est inscrite dans le rapport d'événement Windows à chaque résultat positif. Les événements peuvent être consultés dans l'affichage des événements Windows. Ce paramètre est activé par défaut.

Exceptions

Ces options vous permettent de configurer des objets d'exclusion pour la protection temps réel (recherche en temps réel). Les objets correspondants sont alors ignorés lors de la recherche en temps réel. La protection temps réel peut ignorer via la liste des processus à exclure leurs accès aux fichiers lors de la recherche en temps réel. Ceci est utile notamment pour les bases de données ou solutions de sauvegarde.

Tenez compte de ce qui suit lors de l'indication des processus et objets de fichiers à exclure : la liste est traitée de haut en bas. Plus la liste est longue, plus le temps processeur nécessaire au traitement de la liste pour chaque accès augmente. Gardez la liste aussi courte que possible.

Processus à exclure par la protection temps réel

Tous les accès aux fichiers par les processus de cette liste sont exclus de la surveillance par la protection temps réel.

Champ de saisie

Dans ce champ, saisissez le nom du processus qui doit être ignoré lors de la recherche en temps réel. Aucun processus n'est indiqué par défaut.

Le chemin indiqué et le nom de fichier du processus peuvent contenir 255 signes au maximum. Vous pouvez saisir jusqu'à 128 processus. Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Les caractères Unicode sont acceptés pour indiquer le processus. Vous pouvez par conséquent saisir des noms de processus ou de répertoires contenant des caractères spéciaux.

Les lecteurs doivent être indiqués comme suit : `[lettre du lecteur]:\`

Le caractère deux-points (:) ne peut être utilisé que pour indiquer des lecteurs.

Pour indiquer le processus, vous pouvez utiliser les caractères de remplacement * (un nombre illimité de caractères) et ? (un seul caractère) :

```
C:\Programmes\Application\application.exe
C:\Programmes\Application\applicatio?.exe
C:\Programmes\Application\applica*.exe
C:\Programmes\Application\*.exe
```

Pour éviter d'exclure des processus globalement de la surveillance de la protection temps réel, les indications comprenant exclusivement les caractères suivants ne sont pas valables : * (étoile), ? (point d'interrogation), / (barre oblique), \ (barre oblique inversée), . (point), : (deux-points).

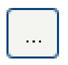
Vous avez la possibilité d'exclure des processus de la surveillance de la protection temps réel sans en indiquer complètement le chemin : `application.exe`

Cela s'applique toutefois exclusivement aux processus dont les fichiers exécutables se trouvent sur les lecteurs du disque dur.

Il est nécessaire d'indiquer complètement le chemin des processus dont les fichiers exécutables se trouvent sur des lecteurs connectés, par ex. des lecteurs réseau. Tenez compte à ce sujet des remarques générales sur l'indication des exceptions sur des lecteurs réseau connectés.

N'indiquez aucune exception pour les processus dont les fichiers exécutables se trouvent sur des lecteurs dynamiques. Les lecteurs dynamiques sont utilisés pour des supports de données tels que des CD, DVD ou clé USB.

Avertissement
Notez que tous les accès aux fichiers initiés par les processus inclus dans la liste sont exclus de la recherche de virus et de programmes indésirables.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner un fichier exécutable.

Processus

Le bouton « **Processus** » ouvre la fenêtre « *Sélection de processus* », dans laquelle les processus en cours sont affichés.



Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le processus entré dans le champ de saisie.

Supprimer

Ce bouton vous permet de supprimer un processus sélectionné de la fenêtre d'affichage.

Objets de fichiers à exclure par la protection temps réel

Tous les accès fichiers aux objets de cette liste sont exclus de la surveillance par la protection temps réel.

Champ de saisie

Entrez dans ce champ le nom de l'objet de fichier qui doit être ignoré par la recherche en temps réel. Aucun objet de fichier n'est indiqué par défaut.

Les entrées de la liste ne doivent pas dépasser 6 000 caractères au total.

Pour indiquer les objets de fichiers à exclure, vous pouvez utiliser les caractères de remplacement * (un nombre illimité de caractères) et ? (un seul caractère). Des extensions de fichiers individuelles peuvent aussi être exclues (y compris avec des caractères de remplacement) :

```
C:\Répertoire\*.mdb
*.mdb
*.md?
*.xls*
C:\Répertoire\*.log
```

Les noms de répertoires doivent se terminer par une barre oblique inversée \.

Lorsqu'un répertoire est exclu, tous ses sous-répertoires sont aussi ignorés automatiquement.

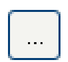
Vous pouvez indiquer 20 exceptions au maximum par lecteur avec le chemin complet (commençant par la lettre du lecteur).

Ex. : `C:\Programmes\Application\Nom.log`

Le nombre maximum d'exceptions sans chemin complet s'élève à 64. Ex. :

```
*.log
 \Ordinateur1\C\Répertoire1
```

Pour les lecteurs dynamiques qui sont connectés (mounted) en tant que répertoire d'un autre lecteur, vous devez utiliser, dans la liste des exceptions, l'alias du système d'exploitation pour le lecteur relié :
ex. `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1`
Si vous utilisez le point de montage (mount point) lui-même, par ex. `C:\DynDrive`, le lecteur dynamique est malgré tout contrôlé. Vous pouvez déterminer l'alias du système d'exploitation à utiliser, à partir du fichier rapport de la protection temps réel.



Ce bouton ouvre une fenêtre dans laquelle vous pouvez sélectionner l'objet de fichier à exclure.

Ajouter

Ce bouton vous permet de reprendre dans la fenêtre d'affichage l'objet de fichier entré dans le champ de saisie.

Supprimer

Le bouton Supprimer vous permet de supprimer un objet de fichier sélectionné de la fenêtre d'affichage.

Tenez compte des autres remarques pour indiquer les exceptions

Pour exclure des objets également lors d'un accès avec un nom de fichier DOS court (convention de noms DOS 8.3), le nom de fichier court correspondant doit aussi être saisi dans la liste.

Un nom de fichier contenant des caractères de remplacement ne doit pas se terminer par une barre oblique inversée.
Par exemple :
`C:\Programmes\Application\applic*.exe\`
Cette entrée n'est pas valable et n'est pas considérée comme une exception.

Tenez compte de ce qui suit pour les **exceptions sur des lecteurs réseau connectés** : si vous utilisez la lettre du lecteur connecté, les fichiers et répertoires indiqués ne sont PAS exclus de la recherche effectuée par la protection temps réel. Si le chemin UNC figurant dans la liste des exceptions est différent de celui utilisé pour connecter le lecteur réseau (indication de l'adresse IP dans la liste des exceptions – indication du nom de l'ordinateur pour la connexion avec le lecteur réseau), les fichiers et répertoires indiqués ne sont PAS exclus de la recherche effectuée par la protection temps réel. Déterminez le chemin UNC à utiliser à l'aide du fichier rapport de la protection temps réel :
`\\<Nom_ordinateur>\<Partage>\` -OU- `\\<Adresse IP>\<Partage>\`

Vous pouvez déterminer les chemins utilisés par la protection temps réel lors de la recherche de fichiers contaminés, à partir du fichier rapport de la protection temps réel. Utilisez systématiquement les mêmes chemins dans la liste des exceptions. Réglez la fonction de consignation de la protection temps réel sur **Intégrale** dans la configuration sous Rapport. La protection temps réel étant activée, accédez maintenant aux fichiers, répertoires, lecteurs intégrés ou lecteurs réseau connectés. Vous pouvez maintenant lire le chemin à utiliser à partir du fichier rapport de la protection temps réel. Vous consultez le fichier rapport dans le Control Center sous Protection temps réel.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche.

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre programme Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.



9.3.2 Rapport

La protection temps réel dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, la protection temps réel ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection temps réel consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection temps réel consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si l'option est activée, la protection temps réel consigne toutes les informations dans le fichier rapport, même celles sur la taille et le type des fichiers, la date, etc.

Limiter le fichier rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier rapport, une marge d'environ 50 kilo-octets est laissée pour ne pas trop solliciter l'ordinateur. Si la taille du fichier rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 50 kilo-octets soit atteinte.

Sauvegarder le fichier rapport avant de le raccourcir

Si l'option est activée, le fichier rapport est sauvegardé avant d'être raccourci.

Mentionner la configuration dans le fichier rapport

Si l'option est activée, la configuration de la recherche en temps réel utilisée est écrite dans le fichier rapport.



> **Remarque**
> Si vous n'avez indiqué aucune limitation du fichier rapport, un nouveau fichier est automatiquement créé lorsque le fichier rapport a atteint une taille de 100 Mo. Une sauvegarde de l'ancien fichier rapport est créée. Jusqu'à trois sauvegardes des anciens fichiers rapport sont conservées. Les sauvegardes les plus anciennes sont supprimées.

9.4 Mise à jour

La rubrique **Mise à jour** vous permet de configurer l'exécution automatique de mises à jour. Vous avez la possibilité de régler différents intervalles de mise à jour.

Mise à jour automatique

tous les n jours / heures / minutes

Dans ce champ, vous pouvez indiquer l'intervalle auquel les mises à jour automatiques doivent être exécutées. Pour modifier l'intervalle de mise à jour, sélectionnez l'une des indications de temps dans le champ et modifiez-la via les touches fléchées à droite du champ de saisie.

Démarrer la tâche en plus à chaque connexion à Internet

Si l'option est activée, en plus de l'intervalle de mise à jour défini, la tâche de mise à jour est exécutée à chaque démarrage d'une connexion Internet.

Reprogrammer la tâche si elle n'a pu être exécutée au moment prévu

Si l'option est activée, le programme effectue les tâches de mise à jour situées dans le passé qui n'ont pas pu être exécutées au moment voulu, par ex. parce que l'ordinateur était éteint.

9.4.1 Serveur Web

Serveur Web

La mise à jour peut être effectuée directement via un serveur Web sur Internet .

Connexion au serveur Web

Utiliser la connexion existante (réseau)

Ce paramètre s'affiche lorsque votre connexion est utilisée via un réseau.

Utiliser la connexion suivante

Ce paramètre s'affiche lorsque vous définissez votre connexion individuellement.

L'Updater détecte automatiquement quelles options de connexion sont disponibles. Les options de connexion indisponibles sont grisées et ne peuvent pas être activées.

Vous pouvez établir une connexion de télétransmission p. ex. manuellement sous Windows par une entrée de répertoire téléphonique.

Utilisateur

Saisissez l'identifiant du compte sélectionné.

Mot de passe

Saisissez le mot de passe pour ce compte. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Remarque
Adressez-vous au fournisseur d'accès Internet si vous avez oublié l'identifiant ou le mot de passe d'un compte Internet existant.

Remarque
La composition automatique de l'Updater via des outils de numérotation (par ex. SmartSurfer, Oleco,...) n'est pas encore disponible.

Arrêter une connexion de télétransmission ouverte pour la mise à jour

Si cette option est activée, la connexion de télétransmission ouverte pour la mise à jour est interrompue automatiquement dès que le téléchargement est terminé.

Remarque
Cette option n'est disponible que sous Windows XP. À partir de Windows Vista, la connexion de télétransmission ouverte pour la mise à jour est systématiquement interrompue, dès que le téléchargement est terminé.

Paramètres proxy

Serveur proxy

Ne pas utiliser de serveur proxy

Si cette option est activée, votre connexion au serveur Web n'a pas lieu via un serveur proxy.

Utiliser les paramètres système de Windows

Si cette option est activée, les paramètres système actuels de Windows pour la connexion au serveur Web via un serveur proxy sont utilisés. Vous configurez les paramètres système de Windows pour l'utilisation d'un serveur proxy sous **Panneau de configuration > Options Internet > Connexions > Paramètres LAN**. Vous pouvez également accéder aux options Internet dans le menu **Extras** d'Internet Explorer.

> **Avertissement**
> Si vous utilisez un serveur proxy qui exige une authentification, indiquez les données complètes sous l'option **Connexion via ce proxy**. L'option **Utiliser les paramètres système de Windows** ne peut être utilisée que pour les serveurs proxy sans authentification.

Connexion via ce serveur proxy

Si l'option est activée, votre connexion au serveur Web a lieu via un serveur proxy, selon les paramètres que vous avez indiqués.

Adresse

Saisissez le nom de l'ordinateur ou l'adresse IP du serveur proxy que vous souhaitez utiliser pour la connexion au serveur Web.

Port

Saisissez le numéro de port du serveur proxy que vous souhaitez utiliser pour la connexion au serveur Web.

Identifiant de connexion

Saisissez un identifiant pour la connexion au serveur proxy.

Mot de passe de connexion

Saisissez le mot de passe correspondant pour la connexion au serveur proxy. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

Exemples :

Adresse : `proxy.domaine.fr` Port : `8080`

Adresse : `192.168.1.100` Port : `3128`

9.5 FireWall

9.5.1 Configuration de l'Avira FireWall

Avira Antivirus Suite vous permet de configurer l'Avira FireWall ou Pare-feu Windows (à partir de Windows 7) :

- Pare-feu Windows

9.5.2 Pare-feu Windows

La rubrique **FireWall** sous **Configuration > Sécurité Internet** permet de configurer Pare-feu Windows dans les systèmes d'exploitation à partir de Windows 7.

Profils réseau

Profils réseau

Pare-feu Windows se base sur les profils réseau pour bloquer l'accès aux programmes et applications non autorisés sur votre ordinateur :

- Réseau privé : pour les réseaux domestiques ou d'entreprise
- Réseau public : pour les réseaux publics
- Réseau avec domaine : pour les réseaux disposant d'un contrôleur de domaine

Vous pouvez gérer ces profils à partir de la configuration de votre produit Avira, sous **Sécurité Internet > Pare-feu Windows > Profils réseau**.

Pour plus d'informations sur ces profils réseau, consultez le site Internet officiel de Microsoft.

> **Avertissement**
> Pare-feu Windows applique les mêmes règles pour tous les réseaux appartenant à un même profil. Ainsi, lorsque vous autorisez un programme ou une application, celui ou celle-ci a également accès à tous les réseaux qui utilisent le même profil.

Réseau privé

Paramètres du réseau privé

Les paramètres du réseau privé gèrent l'accès des autres ordinateurs ou appareils de votre réseau domestique ou d'entreprise à votre ordinateur. Par défaut, ces paramètres permettent aux utilisateurs du réseau privé de voir votre ordinateur et d'y accéder.

Activer

Lorsque cette option est activée, Pare-feu Windows est mis en marche et contrôlé par Avira.

Bloquer toutes les connexions entrantes

Lorsque cette option est activée, Pare-feu Windows refuse toutes les tentatives indésirables de se connecter à votre ordinateur, y compris les connexions entrantes d'applications autorisées.

Me signaliser quand une nouvelle application est bloquée

Lorsque cette option est activée, vous êtes averti chaque fois qu'un programme ou une application est bloqué.

Désactiver (déconseillé)

Cette option désactive Pare-feu Windows. Elle n'est pas recommandée car cela met votre ordinateur en danger.

Réseau public

Paramètres du réseau public

Les paramètres du réseau public gèrent l'accès des autres ordinateurs ou appareils présents dans les réseaux publics à votre ordinateur. Par défaut, ces paramètres ne permettent pas aux utilisateurs du réseau public de voir votre ordinateur et d'y accéder.

Activer

Lorsque cette option est activée, Pare-feu Windows est mis en marche et contrôlé par Avira.

Bloquer toutes les connexions entrantes

Lorsque cette option est activée, Pare-feu Windows refuse toutes les tentatives indésirables de se connecter à votre ordinateur, y compris les connexions entrantes d'applications autorisées.

Me signaliser quand une nouvelle application est bloquée

Lorsque cette option est activée, vous êtes averti chaque fois qu'un programme ou une application est bloqué.

Désactiver (déconseillé)

Cette option désactive Pare-feu Windows. Elle n'est pas recommandée car cela met votre ordinateur en danger.

Réseau avec domaine

Paramètres du réseau avec domaine

Les paramètres du réseau avec domaine gèrent l'accès des autres ordinateurs ou appareils à votre ordinateur lorsque celui-ci est connecté à un réseau authentifié via un contrôleur de domaine. Par défaut, ces paramètres permettent aux utilisateurs authentifiés du domaine de voir votre ordinateur et d'y accéder.

Activer

Lorsque cette option est activée, Pare-feu Windows est mis en marche et contrôlé par Avira.



Bloquer toutes les connexions entrantes

Lorsque cette option est activée, Pare-feu Windows refuse toutes les tentatives indésirables de se connecter à votre ordinateur, y compris les connexions entrantes d'applications autorisées.

Me signaliser quand une nouvelle application est bloquée

Lorsque cette option est activée, vous êtes averti chaque fois qu'un programme ou une application est bloqué.

Désactiver (déconseillé)

Cette option désactive Pare-feu Windows. Elle n'est pas recommandée car cela met votre ordinateur en danger.

Remarque
Cette option est uniquement disponible si votre ordinateur est connecté à un réseau qui dispose d'un contrôleur de domaine.

Règles d'applications

Lorsque vous cliquez sur le lien situé sous **Pare-feu Windows > Règles d'applications**, le menu **Applications et fonctionnalités autorisées** de la configuration de Pare-feu Windows s'affiche.

Paramètres avancés

Lorsque vous cliquez sur le lien situé sous **Pare-feu Windows > Paramètres avancés**, le menu **Pare-feu Windows avec fonctions avancées de sécurité** de la configuration de Pare-feu Windows s'affiche.

9.6 Protection Web

La rubrique **Protection Web** sous **Configuration > Sécurité Internet** sert à la configuration de la protection Web.

9.6.1 Recherche

La protection Web vous protège des virus et logiciels malveillants qui parviennent sur votre ordinateur par le biais des sites Internet que vous chargez dans votre navigateur Internet. Vous pouvez configurer le comportement de la protection Web dans la rubrique **Recherche**.

Recherche

Prise en charge IPv6

Si l'option est activée, la protection Web prend en charge la version 6 du protocole Internet. Cette option n'est pas disponible en cas de nouvelles installations ou modifiées sous Windows 8.

Protection contre les téléchargements automatiques intempestifs

La *protection contre les téléchargements automatiques intempestifs* vous permet de définir des paramètres visant à bloquer les I-Frames, appelées aussi Inline frames. Les I-Frames sont des éléments HTML, c'est-à-dire des éléments de sites Internet qui délimitent une zone d'une page Web. Grâce aux I-Frames, il est possible de charger et d'afficher d'autres contenus Web – le plus souvent d'autres URL – en tant que documents autonomes, dans une sous-fenêtre du navigateur. Les I-Frames sont la plupart du temps utilisées pour les bandeaux publicitaires. Dans certains cas, les I-Frames servent à dissimuler des logiciels malveillants. La zone de l'I-Frame n'est alors le plus souvent que peu ou pas visible dans le navigateur. L'option **Bloquer les I-Frames suspectes** vous permet de contrôler et de bloquer le chargement des I-Frames.

Bloquer les I-Frames suspectes

Si l'option est activée, les I-Frames des sites Internet demandés sont contrôlées selon certains critères. Si des I-Frames suspectes sont présentes sur un site Internet demandé, l'I-Frame est bloquée. Un message d'erreur s'affiche dans la fenêtre de l'I-Frame.

Action si résultat positif

Vous pouvez définir des actions que la protection Web doit exécuter quand un virus ou programme indésirable a été détecté.

Interactif

Si l'option est activée, une boîte de dialogue s'affiche dans laquelle vous pouvez sélectionner ce qui doit advenir du fichier contaminé en cas de détection d'un virus ou d'un programme indésirable pendant la recherche directe. Ce paramètre est activé par défaut.

Afficher la barre de progression

Si l'option est activée, un message affiché sur le Bureau apparaît avec une barre de progression de téléchargement, lorsque le téléchargement de contenus de sites Internet dépasse un délai d'attente de 20 secondes. Ce message affiché sur le Bureau sert notamment à contrôler le téléchargement de sites Internet avec de gros volumes de données : lors de la navigation avec la protection Web, les contenus des sites Internet ne sont pas chargés successivement dans le navigateur Internet, du fait qu'ils sont contrôlés quant à l'absence de virus et de logiciels malveillants avant d'être affichés dans le navigateur. Cette option est désactivée par défaut.

Vous trouverez de plus amples informations ici.

Automatique

Si l'option est activée, aucune boîte de dialogue permettant de sélectionner une action ne s'affiche en cas de détection d'un virus ou d'un programme indésirable. La protection Web réagit en fonction des paramètres réglés dans cette section.

Action primaire

L'action primaire est l'action exécutée lorsque la protection Web trouve un virus ou un programme indésirable.

Refuser l'accès

La page Web demandée par le serveur Web ou les données et fichiers transmis ne sont pas envoyés à votre navigateur Web. Un message d'erreur de refus d'accès s'affiche dans le navigateur Web. La protection Web inscrit le résultat positif dans le fichier rapport, dès lors que la fonction de rapport est activée.

Déplacer en quarantaine

La page Web demandée par le serveur Web ou les données et fichiers transmis sont déplacés en quarantaine en cas de détection d'un virus ou d'un logiciel malveillant. Le fichier concerné peut être restauré depuis le gestionnaire de quarantaines s'il a une valeur informative ou, si nécessaire, être envoyé à l'Avira Malware Research Center.

Ignorer

La page Web demandée par le serveur Web ou les données et fichiers transmis sont envoyés à votre navigateur Web par la protection Web. L'accès au fichier est autorisé et le fichier est conservé.

Avertissement
Le fichier contaminé reste actif sur votre ordinateur. D'importants dégâts peuvent être causés sur votre ordinateur.

Accès bloqués

Sous **Accès bloqués**, vous pouvez indiquer les types de fichiers et les types MIME (types de contenus des données transmises) qui doivent être bloqués par la protection Web. Le filtre Web vous permet de bloquer les URL indésirables et connues, comme par ex. des URL de hameçonnage et de logiciel malveillant. La protection Web empêche la transmission des données depuis Internet vers votre ordinateur.

Types de fichiers / types MIME bloqués par la protection Web

Tous les types de fichiers et les types MIME (types de contenus des données transmises) figurant dans la liste sont bloqués par la protection Web.

Champ de saisie

Saisissez dans ce champ les noms des types MIME et des types de fichiers qui doivent être bloqués par la protection Web. Pour les types de fichiers, saisissez

l'extension de fichier, par ex. **.htm**. Pour les types MIME, notez le type de support et éventuellement le sous-type. Les deux indications sont séparées par une barre oblique, par ex. **video/mpeg** ou **audio/x-wav**.

Remarque
Les fichiers qui ont déjà été enregistrés sur votre ordinateur comme fichiers Internet temporaires sont certes bloqués par la protection Web, mais peuvent être chargés localement par votre ordinateur à partir du navigateur Internet. Les fichiers Internet temporaires sont des fichiers sauvegardés sur votre ordinateur par le navigateur Internet, pour pouvoir afficher plus rapidement les sites Internet.

Remarque
La liste des types de fichiers et types MIME à bloquer est ignorée pour les entrées figurant dans la liste des types de fichiers et types MIME à exclure sous Exceptions.

Remarque
Lorsque vous indiquez des types de fichiers et des types MIME, vous ne pouvez pas utiliser de caractères de remplacement (caractère de remplacement * pour un nombre quelconque de caractères ou ? pour un caractère exactement).

Types MIME : exemples de types de supports

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un programme particulier

Exemples : types de fichiers et types MIME à exclure

- `application/octet-stream` = les fichiers du type MIME application/octet-stream (fichiers exécutables *.bin, *.exe, *.com, *dll, *.class) sont bloqués par la protection Web.
- `application/olescript` = les fichiers du type MIME application/olescript (fichiers script ActiveX *.axs) sont bloqués par la protection Web.
- `.exe` = tous les fichiers avec l'extension .exe (fichiers exécutables) sont bloqués par la protection Web.
- `.msi` = tous les fichiers avec l'extension .msi (fichiers Windows Installer) sont bloqués par la protection Web.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le type MIME ou de fichier entré dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Filtre Web

Le filtre Web dispose d'une base de données interne mise à jour quotidiennement, dans laquelle les URL sont classées par critères de contenus.

Activer le filtre Web

Si l'option est activée, toutes les URL figurant parmi les catégories sélectionnées dans la liste du filtre Web sont bloquées.

Liste du filtre Web

La liste du filtre Web vous permet de choisir les catégories de contenus dont les URL doivent être bloquées par la protection Web.

Remarque
Le filtre Web est ignoré pour les entrées figurant dans la liste des URL à ignorer sous Exceptions.

Remarque
La rubrique **URL de spam** reprend les URL diffusées par des e-mails de spam. La catégorie **Arnaque / fraude** englobe les sites Internet comportant des « pièges d'abonnement » et autres offres de services dont les coûts sont dissimulés par le fournisseur.

Exceptions

Ces options vous permettent d'exclure des types MIME (types de contenus des données transmises) et des types de fichiers d'URL (adresses Internet) de la recherche effectuée par la protection Web. Les types MIME et les URL indiqués sont ignorés par la protection Web, ce qui signifie que ces données ne sont pas contrôlées quant à l'absence de virus et logiciels malveillants, lors de la transmission sur votre ordinateur.

Types MIME à exclure par la protection Web

Dans ce champ, vous pouvez sélectionner les types MIME (types de contenus des données transmises) à exclure de la recherche par la protection Web.

Types de fichiers / types MIME à exclure par la protection Web (définis par l'utilisateur)

Tous les types de fichiers et types MIME (types de contenus des données transmises) figurant dans la liste sont exclus de la recherche par la protection Web.

Champ de saisie

Dans ce champ, vous pouvez indiquer les noms des types MIME et des types de fichiers à exclure de la recherche par la protection Web. Pour les types de fichiers, saisissez l'extension de fichier, par ex. `.htm`. Pour les types MIME, notez le type de support et éventuellement le sous-type. Les deux indications sont séparées par une barre oblique, par ex. `video/mpeg` ou `audio/x-wav`.

> **Remarque**
> Lorsque vous indiquez des types de fichiers et des types MIME, vous ne pouvez pas utiliser de caractères de remplacement (caractère de remplacement * pour un nombre quelconque de caractères ou ? pour un caractère exactement).

> **Avertissement**
> Tous les types de fichiers et de contenus figurant sur la liste d'exclusion sont chargés dans le navigateur Internet sans contrôle additionnel des accès bloqués (liste des types fichiers et types MIME à bloquer sous Accès bloqués) ou de la protection Web : pour toutes les entrées figurant sur la liste d'exclusion, les entrées de la liste des types de fichiers et types MIME à bloquer sont ignorées. Aucune recherche de virus et de logiciels malveillants n'est effectuée.

Types MIME : exemples de types de supports

- `text` = pour fichiers texte
- `image` = pour fichiers graphiques
- `video` = pour fichiers vidéo
- `audio` = pour fichiers son
- `application` = pour les fichiers associés à un programme particulier

Exemples : types de fichiers et types MIME à exclure

- `audio/` = tous les fichiers de type audio sont exclus de la recherche effectuée par la protection Web
- `video/quicktime` = tous les fichiers vidéo du sous-type Quicktime (*.qt, *.mov) sont exclus de la recherche effectuée par la protection Web
- `.pdf` = tous les fichiers PDF Adobe sont exclus de la recherche effectuée par la protection Web.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage le type MIME ou de fichier entré dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

URL à exclure par la protection Web

Toutes les URL de cette liste sont exclues de la recherche effectuée par la protection Web.

Champ de saisie

Saisissez dans ce champ les URL (adresses Internet) à exclure de la recherche par la protection Web, par ex. **www.nomdedomaine.com**. Vous pouvez indiquer des parties de l'URL en signalant le niveau de domaine avec des points finaux ou de début : nomdedomaine.fr pour tous les sites et tous les sous-domaines du domaine. Notez un site Web avec un domaine de niveau supérieur quelconque (.com ou .net) avec un point final : **nomdedomaine.**. Si vous notez une suite de caractères sans point final ou point de début, celle-ci sera interprétée comme un domaine de niveau supérieur, par ex. **net** pour tous les domaines NET (www.domaine.net).

Remarque
Lors de l'indication des URL, vous pouvez également utiliser le caractère de remplacement * pour un nombre quelconque de caractères. Utilisez aussi des points finaux ou de début en combinaison avec les caractères de remplacement, pour repérer les niveaux de domaine :
`nomdedomaine.*`
`*.nomdedomaine.com`
`.*nom*.com` (applicable mais pas recommandé)
Les indications sans points comme `*nom*` sont interprétées comme des parties d'un domaine de niveau supérieur et ne sont donc pas judicieuses.

Avertissement
Tous les sites Web figurant sur la liste des URL à exclure sont chargés dans le navigateur Internet sans contrôle additionnel de la part du filtre Web ou de la protection Web : pour toutes les entrées figurant dans la liste des URL à exclure, les entrées du filtre Web sont ignorées (voir Accès bloqués). Aucune recherche de virus et de logiciels malveillants n'est effectuée. Par conséquent, n'excluez de la recherche par la protection Web que les URL dignes de confiance.

Ajouter

Ce bouton vous permet de valider dans la fenêtre d'affichage l'URL (adresse Internet) entrée dans le champ de saisie.

Supprimer

Le bouton supprime une entrée sélectionnée de la liste. Ce bouton n'est pas actif si aucune entrée n'est sélectionnée.

Exemples : URL à exclure

- `www.avira.com` -OU- `www.avira.com/*`
  = toutes les URL avec le domaine www.avira.com sont exclues de la recherche effectuée par la protection Web : www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,...
  Les URL avec le domaine www.avira.fr ne sont pas exclues de la recherche effectuée par la protection Web.
- `avira.com` -OU- `*.avira.com`
  = toutes les URL avec le domaine de second niveau et de niveau supérieur avira.com sont exclues de la recherche effectuée par la protection Web. L'indication implique tous les sous-domaines existants pour .avira.com : www.avira.com, forum.avira.com,...
- `avira.` -OU- `*.avira.*`
  = toutes les URL avec le domaine de second niveau avira sont exclues de la recherche effectuée par la protection Web. L'indication implique tous les domaines de niveau supérieur ou les sous-domaines existants pour .avira. : www.avira.com, www.avira.fr, forum.avira.com,...
- `.*domain*.*`
  = toutes les URL contenant un domaine de second niveau avec la chaîne de caractères domain sont exclues de la recherche effectuée par la protection Web : www.domain.com, www.new-domain.fr, www.sample-domain1.fr, ...
- `net` -OU- `*.net`
  = toutes les URL avec le domaine de niveau supérieur net sont exclues de la recherche effectuée par la protection Web : www.name1.net, www.name2.net,...

Avertissement
Indiquez aussi précisément que possible les URL que vous souhaitez exclure de la recherche effectuée par la protection Web. Évitez d'indiquer des ensembles de domaines de niveau supérieur ou des parties d'un nom de domaine de second niveau, car il y a un risque que des pages Internet propageant des logiciels malveillants ou programmes indésirables soient exclues de la recherche effectuée par la protection Web par des indications globales définies sous la rubrique Exceptions. Il est recommandé d'indiquer au moins le domaine de second niveau entièrement et le domaine de niveau supérieur : nomdedomaine.com

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche.

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre produit Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

9.6.2 Rapport

La protection Web dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, la protection Web ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection Web consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection Web consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si cette option est activée, la protection Web consigne toutes les informations dans le fichier rapport, même celles sur la taille et le type des fichiers, la date, etc.

Limiter le fichier rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier rapport, une marge d'environ 50 kilo-octets est laissée pour ne pas trop solliciter l'ordinateur. Si la taille du fichier rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 20 % soit atteinte.

Écrire la configuration dans le fichier rapport

Si l'option est activée, la configuration de la recherche en temps réel utilisée est écrite dans le fichier rapport.

Remarque
Si vous n'avez indiqué aucune limitation du fichier rapport, les anciennes



entrées sont automatiquement supprimées lorsque le fichier rapport a atteint une taille de 100 Mo. Les entrées sont supprimées tant que le fichier rapport n'a pas atteint une taille de 80 Mo.

9.7 Protection e-mail

La rubrique Protection e-mail de la configuration permet de configurer la protection e-mail.

9.7.1 Recherche

Vous utilisez la protection e-mail pour contrôler les e-mails entrants quant à l'absence de virus, de logiciels malveillants . Il est possible de faire contrôler les e-mails sortants par la protection e-mail quant à l'absence de virus et de logiciels malveillants.

Contrôler les e-mails entrants

Si l'option est activée, les e-mails entrants sont contrôlés quant à l'absence de virus, de logiciels malveillants. La protection e-mail prend en charge les protocoles POP3 et IMAP. Activez le compte de la boîte de réception utilisé par votre client de messagerie pour la réception des e-mails, pour le faire surveiller par la protection e-mail.

Surveiller les comptes POP3

Si l'option est activée, les comptes POP3 sont surveillés sur les ports indiqués.

Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte de réception par le protocole POP3. Vous pouvez indiquer plusieurs ports en les séparant par des virgules.

Par défaut

Ce bouton permet de réinitialiser les ports indiqués au port POP3 par défaut.

Surveiller les comptes IMAP

Si l'option est activée, les comptes IMAP sont surveillés sur les ports indiqués.

Ports surveillés

Saisissez dans ce champ le port utilisé par le protocole IMAP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules.

Par défaut

Ce bouton permet de réinitialiser les ports indiqués au port IMAP par défaut.

Contrôler les e-mails sortants (SMTP)

Si l'option est activée, les e-mails sortants sont contrôlés quant à l'absence de virus et de logiciels malveillants.



Ports surveillés

Saisissez dans ce champ le port utilisé comme boîte d'envoi par le protocole SMTP. Vous pouvez indiquer plusieurs ports en les séparant par des virgules.

Par défaut

Ce bouton permet de réinitialiser les ports indiqués au port SMTP par défaut.

> **Remarque**
> Pour vérifier les protocoles et les ports utilisés, consultez les propriétés de vos comptes dans votre programme client de messagerie électronique. Les ports par défaut sont ceux qui sont utilisés par la majorité des comptes de messagerie.

Prise en charge IPv6

Si l'option est activée, la protection e-mail prend en charge la version 6 du protocole Internet. (Option non disponible en cas de nouvelles installations ou modifiées sous Windows 8.)

Action si résultat positif

Cette rubrique de configuration contient des paramètres concernant les actions effectuées lorsque la protection e-mail trouve un virus ou un programme indésirable dans un e-mail ou une pièce jointe.

> **Remarque**
> Les actions définies ici sont exécutées en cas de détection de virus dans des e-mails entrants, de même que dans des e-mails sortants.

Interactif

Si l'option est activée, une boîte de dialogue s'affiche pour sélectionner l'action à effectuer avec le fichier contaminé ou la pièce jointe en cas de détection d'un virus ou d'un programme indésirable dans un e-mail ou une pièce jointe. Cette option est activée par défaut.

Afficher la barre de progression

Si l'option est activée, la protection e-mail affiche une barre de progression pendant le téléchargement des e-mails. L'activation de cette option n'est possible que si l'option **Interactif** a été sélectionnée.

Automatique

Si l'option est activée, vous n'êtes plus prévenu si un virus ou un programme indésirable est détecté. La protection e-mail réagit en fonction des paramètres définis dans cette section.

E-mails contaminés

L'option choisie sous « *E-mails contaminés* » est exécutée en tant qu'action primaire si la protection e-mail trouve un virus ou un programme indésirable dans un e-mail. Si l'option « **Ignorer** » est sélectionnée, vous pouvez choisir sous « *Pièces jointes contaminées* **»** ce qui doit se passer quand un résultat positif est détecté dans une pièce jointe.

Supprimer

Si cette option est activée, l'e-mail contaminé est automatiquement supprimé si un virus ou un programme indésirable a été détecté. Le corps de l'e-mail (body) est remplacé par le texte standard ci-dessous. La même chose s'applique à toutes les pièces jointes (attachments) ; celles-ci sont également remplacées par un texte standard.

Ignorer

Si l'option est activée, l'e-mail contaminé est ignoré même si un virus ou un programme indésirable a été détecté. Vous avez toutefois la possibilité de décider ce qui doit advenir d'une pièce jointe contaminée.

Déplacer en quarantaine

Si l'option est activée, l'e-mail complet avec toutes ses pièces jointes est mis en Quarantaine si un virus ou un programme indésirable est détecté. Il peut être restauré ensuite sur demande. L'e-mail contaminé lui-même est supprimé. Le corps de l'e-mail (body) est remplacé par le texte standard ci-dessous. La même chose s'applique à toutes les pièces jointes (attachments) ; celles-ci sont également remplacées par un texte standard.

Pièces jointes contaminées

L'option « **Pièces jointes contaminées** » ne peut être sélectionnée que si, sous « *E-mails contaminés* **»**, l'option « **Ignorer** » a été sélectionnée. Cette option permet de décider ce qui doit être fait si une pièce jointe est contaminée.

Supprimer

Si l'option est activée, la pièce jointe contaminée par un virus ou un programme indésirable est supprimée et remplacée par un texte standard.

Ignorer

Si l'option est activée, la pièce jointe contaminée est ignorée et délivrée même si un virus ou un programme indésirable a été détecté.

Avertissement
Si vous choisissez cette option, vous n'êtes pas du tout protégé des virus et programmes indésirables par la protection e-mail. Ne choisissez cette rubrique que si vous savez exactement ce que vous faites. Désactivez l'aperçu dans votre programme de messagerie électronique, n'ouvrez pas les pièces jointes par double-clic.

Déplacer en quarantaine

Si cette option est activée, la pièce jointe contaminée est placée en quarantaine puis supprimée (remplacée par un texte standard). La pièce jointe contaminée peut être restaurée ensuite, sur demande.

Autres actions

Cette rubrique de configuration contient d'autres paramètres concernant les actions effectuées lorsque la protection e-mail trouve un virus ou un programme indésirable dans un e-mail ou une pièce jointe.

> **Remarque**
> Les actions définies ici sont exécutées exclusivement en cas de détection de virus dans des e-mails entrants.

Texte standard pour les e-mails supprimés et déplacés

Le texte dans ce champ est ajouté comme message dans l'e-mail, à la place de l'e-mail contaminé. Vous pouvez modifier ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour la mise en forme :

Ctrl + Enter = ajoute un saut de ligne.

Par défaut

Le bouton insère un texte standard prédéfini dans le champ d'édition.

Texte standard pour les pièces jointes supprimées et déplacées

Le texte de ce champ est ajouté comme message dans l'e-mail, à la place de la pièce jointe contaminée. Vous pouvez modifier ce message. Un texte ne doit pas contenir plus de 500 caractères.

Vous pouvez utiliser les combinaisons de touches suivantes pour la mise en forme :

Ctrl + Enter = ajoute un saut de ligne.

Par défaut

Le bouton insère un texte standard prédéfini dans le champ d'édition.

Heuristique

Cette rubrique de configuration contient les paramètres pour l'heuristique du moteur de recherche.

Les produits Avira contiennent des heuristiques très performantes qui permettent de détecter dynamiquement des logiciels malveillants inconnus, c'est-à-dire avant même qu'une signature de virus spéciale n'ait été créée contre le parasite et qu'une mise à jour de protection antivirus correspondante n'ait été envoyée. La détection des virus s'effectue

par une analyse complexe et un examen du code en cause, à la recherche de fonctions typiques des logiciels malveillants. Si le code examiné présente ces caractéristiques, il est signalé comme suspect. Cela ne signifie pas obligatoirement que le code est un logiciel malveillant ; des messages erronés peuvent aussi survenir. C'est l'utilisateur qui doit décider comment traiter le code, par ex. sur la base de ses connaissances pour savoir si la source contenant le code signalé est digne de confiance.

Heuristique de macrovirus

Votre produit Avira contient une heuristique de macrovirus très performante. Si l'option est activée, toutes les macros du document contaminé sont supprimées si une réparation est possible ; les documents suspects peuvent aussi être seulement signalés, c'est-à-dire que vous recevez un avertissement. Ce paramètre est activé par défaut et recommandé.

Advanced Heuristic Analysis and Detection (AHeAD)

Activer AHeAD

Votre produit Avira contient une heuristique très performante grâce à la technologie Avira AHeAD, lui permettant de détecter aussi les (nouveaux) logiciels malveillants inconnus. Si l'option est activée, vous pouvez régler ici la sensibilité de cette heuristique. Ce paramètre est activé par défaut.

Niveau de détection bas

Si l'option est activée, moins de logiciels malveillants inconnus sont détectés, le risque de détections erronées est faible dans ce cas.

Niveau de détection moyen

Si l'option est activée, une protection équilibrée est assurée avec peu de messages d'erreurs. Ce paramètre est activé par défaut si vous avez choisi l'utilisation de cette heuristique.

Niveau de détection élevé

Si l'option est activée, nettement plus de logiciels malveillants inconnus sont détectés, sachant qu'il faut toutefois s'attendre à des messages erronés.

9.7.2 Généralités

Exceptions

Adresses e-mail qui ne sont pas contrôlées

Ce tableau vous donne la liste des adresses e-mail qui ont été exclues du contrôle effectué par la protection e-mail d'Avira (liste blanche).



Remarque
La liste des exceptions est utilisée par la protection e-mail exclusivement pour les e-mails entrants.

Adresses e-mail qui ne sont pas contrôlées

Champ de saisie

Saisissez dans ce champ l'adresse e-mail que vous souhaitez ajouter à la liste des adresses e-mail à ne pas contrôler. L'adresse e-mail ne sera dorénavant plus contrôlée par la protection e-mail, en fonction de vos paramètres.

Ajouter

Ce bouton vous permet d'ajouter à la liste des adresses e-mail à ne pas contrôler l'adresse e-mail entrée dans le champ de saisie.

Supprimer

Ce bouton supprime l'adresse e-mail sélectionnée dans la liste.

Adresse e-mail

Adresse e-mail qui ne doit plus être contrôlée.

Logiciels malveillants

Si l'option est activée, l'adresse e-mail ne sera plus contrôlée quant à la présence de logiciels malveillants.

Vers le haut

Ce bouton vous permet de déplacer une adresse e-mail sélectionnée d'une position vers le haut. Ce bouton n'est pas disponible si aucune entrée n'est sélectionnée ou si l'adresse sélectionnée figure en première position dans la liste.

Vers le bas

Ce bouton vous permet de déplacer une adresse e-mail sélectionnée d'une position vers le bas. Ce bouton n'est pas disponible si aucune entrée n'est sélectionnée ou si l'adresse sélectionnée figure en dernière position dans la liste.

Mémoire tampon

La mémoire tampon de la protection e-mail contient les données sur les e-mails contrôlés qui sont affichés dans les statistiques du Control Center sous **Protection e-mail**.

Nombre maximum d'e-mails dans la mémoire tampon

Saisissez dans ce champ le nombre maximum d'e-mails conservés dans la mémoire tampon de la protection e-mail. Les e-mails les plus anciens sont supprimés.

Durée de mémorisation maximale d'un e-mail en jours

Saisissez dans ce champ la durée de mémorisation maximale d'un e-mail en jours. Après cet intervalle, l'e-mail est supprimé de la mémoire tampon.

Vider la mémoire tampon

Cliquez sur ce bouton pour supprimer les e-mails conservés dans la mémoire tampon.

9.7.3 Rapport

La protection e-mail dispose d'une fonction étendue de consignation qui peut donner à l'utilisateur et à l'administrateur des indications exactes sur un résultat positif.

Consignation

Ce groupe permet de définir le contenu du fichier rapport.

Désactivée

Si l'option est activée, la protection e-mail ne génère pas de rapport.
Ne renoncez à la consignation que dans des cas exceptionnels, par ex. uniquement lorsque vous effectuez des tests avec de nombreux virus ou programmes indésirables.

Par défaut

Si l'option est activée, la protection e-mail consigne les informations importantes (sur les résultats positifs, les avertissements et les erreurs) dans le fichier rapport, les informations secondaires sont ignorées pour une meilleure lisibilité. Ce paramètre est activé par défaut.

Étendue

Si l'option est activée, la protection e-mail consigne également les informations secondaires dans le fichier rapport.

Intégrale

Si cette option est activée, la protection e-mail consigne toutes les informations dans le fichier rapport.

Limiter le fichier rapport

Limiter la taille à n Mo

Si l'option est activée, il est possible de limiter la taille du fichier rapport ; valeurs possibles : 1 à 100 Mo. En cas de limitation du fichier rapport, une marge d'environ 50 kilo-octets est laissée pour ne pas trop solliciter l'ordinateur. Si la taille du fichier rapport dépasse la taille indiquée de 50 kilo-octets, les anciennes entrées sont supprimées automatiquement jusqu'à ce que la taille indiquée moins 50 kilo-octets soit atteinte.

Sauvegarder le fichier rapport avant de le raccourcir

Si l'option est activée, le fichier rapport est sauvegardé avant d'être raccourci.

Écrire la configuration dans le fichier rapport

Si l'option est activée, la configuration utilisée par la protection e-mail est inscrite dans le fichier rapport.

Remarque
Si vous n'avez indiqué aucune limitation du fichier rapport, un nouveau fichier est automatiquement créé lorsque le fichier rapport a atteint une taille de 100 Mo. Une sauvegarde de l'ancien fichier rapport est créée. Jusqu'à trois sauvegardes des anciens fichiers rapport sont conservées. Les sauvegardes les plus anciennes sont supprimées.

9.8 Généralités

9.8.1 Catégories de dangers

Sélection de catégories de dangers étendues

Votre produit Avira vous protège des virus informatiques. En outre, vous avez la possibilité d'effectuer différentes recherches selon les catégories de dangers suivantes.

- Logiciels publicitaires
- Logiciels publicitaires/logiciels espions
- Applications
- Logiciels de commande Backdoor
- Fichiers à extensions déguisées
- Programmes de numérotation payants
- Hameçonnage
- Programmes portant atteinte à la vie privée
- Programmes de blagues
- Jeux
- Logiciels frauduleux
- Logiciels de compression inhabituels

Cliquez sur la case correspondante pour activer le type sélectionné (coché) ou le désactiver (décoché).

Activer tout

Si l'option est activée, tous les types sont activés.

Valeurs par défaut

Ce bouton restaure les valeurs définies par défaut.

Remarque
Si un type est désactivé, les fichiers identifiés comme type de programme correspondant ne sont plus signalés. En outre, aucune entrée n'est ajoutée au fichier rapport.

9.8.2 Protection étendue

Protection étendue

ProActiv

Activer la fonction ProActiv

Si l'option est activée, les programmes de votre ordinateur sont surveillés et examinés pour savoir s'ils exécutent des actions suspectes. En cas de comportement typique de logiciels malveillants, vous êtes averti par un message. Vous avez la possibilité de bloquer le programme ou de poursuivre son exécution à l'aide de l'option « **Ignorer** ». Sont exclus de la surveillance : les programmes classifiés comme étant dignes de confiance, les programmes signés et dignes de confiance figurant par défaut dans le filtre des applications autorisées, tous les programmes que vous avez ajoutés au filtre des programmes autorisés.

En utilisant la fonction ProActiv, vous vous protégez contre les nouvelles menaces et les menaces inconnues pour lesquelles il n'existe encore aucune définition de virus ni heuristique. La technologie ProActiv, intégrée au composant Protection temps réel, observe et analyse les actions exécutées par des programmes. Le comportement de programmes est examiné à la recherche de modèles d'action typiques d'un logiciel malveillant : type d'action et séquences de l'action. Si un programme a un comportement typique d'un logiciel malveillant, celui-ci est traité et signalé comme un résultat positif de virus : vous avez la possibilité de bloquer l'exécution du programme ou d'ignorer le message et de poursuivre l'exécution du programme. Vous pouvez classer le programme comme étant digne de confiance et l'ajouter ainsi au filtre des programmes autorisés. Vous avez également la possibilité d'ajouter le programme au filtre des programmes à bloquer via l'instruction **Toujours bloquer**.

Pour déterminer s'il s'agit d'un comportement suspect, le composant ProActiv utilise un ensemble de règles mises au point par le centre de recherche sur les logiciels malveillants Avira Malware Research Center. Les ensembles de règles sont alimentés par les bases de données Avira. Pour la saisie d'informations dans les bases de données Avira, ProActiv envoie des informations sur les programmes signalés comme suspects. Au cours de

l'installation d'Avira, vous pouvez désactiver la transmission de données aux bases de données Avira.

> **Remarque**
> La technologie ProActiv n'est pas encore disponible sur les systèmes 64 bits.

Protection Cloud

Activer la protection Cloud

Les empreintes de tous les fichiers suspects sont transmises au Cloud d'Avira pour la détection en ligne dynamique. Les fichiers d'applications sont aussitôt identifiés comme étant sains, contaminés ou inconnus.

Le système de protection Cloud sert de nœud central pour détecter les cyber-attaques à l'encontre de la communauté Avira. Les fichiers auxquels votre PC accède sont comparés avec des modèles de fichiers enregistrés dans le système de Cloud. L'essentiel du travail ayant lieu dans le Cloud, le programme de protection local a besoin de moins de ressources.

Une liste des emplacements d'enregistrement des fichiers ciblés par le logiciels malveillants est établie à chaque **contrôle rapide du système**. Dans cette liste figurent par exemple les processus, les programmes de démarrage et les programmes de services en cours. Une somme de contrôle numérique (« empreinte ») est créée à partir de chaque fichier ; elle est envoyée au système de protection Cloud, pour être ensuite identifiée comme « saine » ou « logiciel malveillant ». Les fichiers de programmes inconnus sont chargés dans le système de protection Cloud en vue de leur analyse.

Confirmer manuellement en cas d'envoi de fichiers suspects à Avira

Vous pouvez contrôler la liste des fichiers suspects qui doivent être envoyés à la protection Cloud et choisir vous-même les fichiers que vous souhaitez charger.

Scan des fichiers en temps réel

Si cette option est activée, les fichiers inconnus sont envoyés au Protection Cloud pour être analysés dès leur accès.

Afficher la progression des chargements vers le Protection Cloud Avira

Une fenêtre affiche les informations suivantes concernant les fichiers chargés sous forme de barre de progression :

- emplacement du fichier

- nom du fichier

- état (chargement/analyse)

- résultat (propre/infecté)

Sous *Applications à bloquer*, vous pouvez ajouter les applications que vous considérez comme nuisibles et qui doivent être bloquées par défaut par Avira ProActiv. Les applications ajoutées ne peuvent pas être exécutées sur votre système informatique. Vous pouvez également ajouter des programmes au filtre des applications à bloquer via les messages de la protection temps réel concernant le comportement suspect d'un programme en utilisant l'option **Toujours bloquer ce programme** .

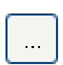
Applications à bloquer

Application

La liste reprend toutes les applications que vous avez classées comme étant nuisibles et que vous avez ajoutées via la configuration ou via les messages du composant ProActiv. Les applications de la liste sont bloquées par Avira ProActiv et ne peuvent pas être exécutées sur votre système informatique. Lors du démarrage d'un programme à bloquer, un message du système d'exploitation s'affiche. Avira ProActiv identifie les applications à bloquer à l'aide du chemin indiqué et du nom de fichier et les bloque indépendamment de leur contenu.

Champ de saisie

Saisissez dans ce champ l'application qui doit être bloquée. Pour identifier l'application, il faut indiquer le chemin complet et le nom de fichier avec son extension. L'indication de chemin doit soit contenir le lecteur sur lequel se trouve l'application, soit commencer avec une variable d'environnement.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner l'application à bloquer.

Ajouter

Le bouton « **Ajouter** » vous permet de reprendre dans la liste des applications à bloquer, l'application indiquée dans le champ de saisie.

> **Remarque**
> Les applications nécessaires au fonctionnement du système d'exploitation ne peuvent être ajoutées à la liste.

Supprimer

Le bouton « **Supprimer** » vous permet de supprimer une application sélectionnée de la liste des applications à bloquer.

Sous *Applications à exclure*, sont énumérées les applications qui sont exclues de la surveillance du composant ProActiv : les programmes signés classifiés comme dignes de confiance et figurant par défaut dans la liste, toutes les applications que vous considérez comme étant dignes de confiance et que vous ajoutez dans le filtre des applications : dans la configuration, vous pouvez ajouter des applications à la liste des applications

autorisées. Vous pouvez également ajouter des applications via les messages de la protection temps réel concernant le comportement suspect d'un programme, en utilisant l'option **Programme digne de confiance** dans le message de la protection temps réel.

Applications à exclure

Application

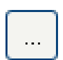
La liste contient les applications exclues de la surveillance du composant ProActiv. Dans les paramètres par défaut après l'installation, la liste contient les applications signées de fabricants dignes de confiance. Vous avez la possibilité d'ajouter les applications que vous avez classifiées comme étant dignes de confiance via la configuration ou via les messages de la protection temps réel. Le composant ProActiv identifie les applications à l'aide du chemin, du nom de fichier et du contenu. Un contrôle de contenu est judicieux car il est possible d'ajouter ultérieurement à un programme un code malveillant via des modifications telles que des mises à jour. Le **type** indiqué vous permet de déterminer la manière dont le contenu doit être contrôlé : avec le type « *Contenu* », les applications indiquées avec le chemin et le nom de fichier sont examinées pour voir si le contenu du fichier ne présente pas des modifications, avant d'être exclues de la surveillance par le composant ProActiv. En cas de modification du contenu du fichier, l'application est à nouveau surveillée par le composant ProActiv. Avec le type « *Chemin* », il n'y a pas de contrôle du contenu avant que l'application ne soit exclue de la surveillance effectuée par la protection temps réel. Pour changer le type d'exclusion, cliquez sur le type affiché.

Avertissement
Utilisez le type *Chemin* uniquement dans des cas exceptionnels. Une mise à jour peut permettre d'ajouter un code malveillant à une application. L'application à l'origine inoffensive devient alors un logiciel malveillant.

Remarque
Quelques applications dignes de confiance comme p. ex. tous les composants d'application de votre produit Avira, sont exclus par défaut d'une surveillance par le composant ProActiv, mais ne figurent pas sur la liste.

Champ de saisie

Dans ce champ, vous indiquez l'application devant être exclue de la surveillance par le composant ProActiv. Pour identifier l'application, il faut indiquer le chemin complet et le nom de fichier avec son extension. L'indication de chemin doit soit contenir le lecteur sur lequel se trouve l'application, soit commencer avec une variable d'environnement.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner l'application à exclure.

Ajouter

Le bouton « **Ajouter** » vous permet de reprendre dans la liste des applications à exclure, l'application indiquée dans le champ de saisie.

Supprimer

Le bouton « **Supprimer** » vous permet de supprimer une application sélectionnée de la liste des applications à exclure.

9.8.3 Mot de passe

Vous pouvez protéger votre produit Avira dans diverses zones par un mot de passe. Si un mot de passe a été attribué, vous devez saisir ce mot de passe à chaque fois que vous voulez ouvrir la zone protégée.

Mot de passe

Saisir le mot de passe

Saisissez ici le mot de passe de votre choix. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*). Vous pouvez saisir 20 caractères au maximum. Si le mot de passe est indiqué une fois, le programme refuse l'accès en cas de saisie d'un mot de passe erroné. Un champ vide signifie « Aucun mot de passe ».

Confirmation

Saisissez ici de nouveau le mot de passe indiqué ci-dessus pour le confirmer. Pour des raisons de sécurité, les véritables caractères saisis dans ce champ sont remplacés par des astérisques (*).

> **Remarque**
> Le mot de passe est sensible à la casse.

Zones protégées par mot de passe

Votre produit Avira peut protéger diverses zones par mot de passe. En cliquant sur la case correspondante, la demande de mot de passe pour les diverses zones peut être désactivée et activée à volonté.

Zone protégée par mot de passe	Fonction
Control Center	Si l'option est activée, le mot de passe défini est nécessaire pour le démarrage du Control Center.
Activer / désactiver la protection temps réel	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection temps réel Avira.
Activer / désactiver la protection e-mail	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection e-mail.
Activer / désactiver la protection Web	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver la protection Web.
Quarantaine	Si l'option est activée, le mot de passe défini est nécessaire pour activer et désactiver toutes les zones du gestionnaire de quarantaines. En cliquant sur la case correspondante, la demande de mot de passe peut être désactivée et activée à volonté.
Restauration des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour restaurer un objet.
Nouveau contrôle des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour contrôler à nouveau un objet.
Propriétés des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour afficher les propriétés d'un objet.
Suppression des objets concernés	Si l'option est activée, le mot de passe défini est nécessaire pour supprimer un objet.
Envoyer un e-mail à Avira	Si l'option est activée, le mot de passe défini est nécessaire pour envoyer un objet à l'Avira Malware Research Center pour contrôle.

Ajout et modification des tâches	Si l'option est activée, le mot de passe défini est nécessaire pour ajouter et modifier des tâches dans le planificateur.
Configuration	Si l'option est activée, la configuration du programme n'est possible qu'après saisie du mot de passe défini.
Installation / désinstallation	Si l'option est activée, le mot de passe défini est nécessaire pour installer et désinstaller le programme.

9.8.4 Sécurité

Autorun

Bloquer la fonction Autorun

Si l'option est activée, l'exécution de la fonction Autorun de Windows est bloquée sur tous les lecteurs intégrés comme les clés USB, les lecteurs de CD et DVD, les lecteurs réseau. Avec la fonction Autorun de Windows, les fichiers sur des supports de données ou sur des lecteurs réseau sont immédiatement lus lors de l'insertion ou de la connexion. Ainsi, les fichiers peuvent être démarrés et reproduits automatiquement. Cette fonctionnalité implique toutefois un risque élevé pour la sécurité, car des logiciels malveillants ou programmes indésirables peuvent être installés en cas de démarrage automatique des fichiers. La fonction Autorun est particulièrement critique pour les clés USB car les données d'une clé USB peuvent constamment changer.

Exclure les CD et DVD

Si l'option est activée, la fonction Autorun est autorisée sur les lecteurs de CD et DVD.

Avertissement
Ne désactivez la fonction Autorun pour les lecteurs de CD et DVD que si vous êtes certain d'utiliser uniquement des supports de données fiables.

Protection système

Protéger le fichier hôte Windows des modifications

Si cette option est activée, le fichier hôte Windows est protégé en écriture. Il n'est plus possible de manipuler le fichier. Les logiciels malveillants ne sont plus capables, par exemple, de vous rediriger sur des pages Internet non souhaitées. Cette option est activée par défaut.

Protection du produit

Remarque
Les options de protection du produit ne sont pas disponibles si la protection temps réel n'a pas été installée lors d'une installation personnalisée.

Protéger les processus d'un arrêt non souhaité

Si l'option est activée, tous les processus du programme sont protégés d'un arrêt non souhaité par des virus et des logiciels malveillants ou d'un arrêt « incontrôlé » par un utilisateur, par ex. via le gestionnaire des tâches. Cette option est activée par défaut.

Protection étendue des processus

Si l'option est activée, tous les processus du programme sont protégés par des méthodes avancées contre un arrêt non souhaité. La protection étendue des processus utilise beaucoup plus de ressources que la protection simple des processus. L'option est activée par défaut. Un redémarrage de l'ordinateur est nécessaire pour désactiver l'option.

Remarque
La protection de processus n'est pas disponible sous Windows XP 64 bits !

Avertissement
Si la protection des processus est activée, des problèmes d'interaction peuvent survenir avec d'autres logiciels. Désactivez la protection des processus dans ces cas.

Protéger les fichiers et entrées de Registre de toute manipulation

Si l'option est activée, toutes les entrées de Registre du programme, ainsi que tous les fichiers (fichiers binaires et de configuration) sont protégés contre toute manipulation. La protection contre la manipulation comprend la protection contre l'accès en écriture, en suppression et partiellement en lecture aux entrées de Registre ou aux fichiers du programme, par l'utilisateur ou des programmes-tiers. Pour activer l'option, il est nécessaire de redémarrer l'ordinateur.

Avertissement
Veuillez noter que si l'option est désactivée, il se peut que la réparation des ordinateurs contaminés par certains types de logiciels malveillants échoue.

Remarque
Si l'option est activée, les modifications de la configuration ne sont possibles que via l'interface utilisateur, de même que la modification des tâches de contrôle ou de mise à jour.

Remarque
La protection des fichiers et des entrées de Registre n'est pas disponible sous Windows XP 64 bits !

9.8.5 WMI

Prise en charge de Windows Management Instrumentation (WMI)

Windows Management Instrumentation est une technologie de gestion Windows de base qui permet d'accéder en lecture et en écriture aux paramètres d'ordinateurs Windows, localement et à distance, au moyen de langages de script et de programmation. Votre produit Avira prend en charge WMI et met à disposition d'une interface, les données (informations sur l'état, données statistiques, rapports, tâches planifiées, etc.) ainsi que les événements . WMI vous donne la possibilité de consulter les données d'exploitation du programme.

Activer la prise en charge WMI

Si l'option est activée, vous avez la possibilité de consulter les données d'exploitation du programme via WMI.

9.8.6 Événements

Limiter la taille de la base de données d'événements

Limiter la taille à n entrées maximum

Si l'option est activée, le nombre maximum d'entrées dans la base de données d'événements peut être limité à une taille définie ; les valeurs autorisées sont : 100 à 10 000 entrées. Si le nombre d'entrées saisies est dépassé, les saisies les plus anciennes sont supprimées.

Supprimer tous les événements de plus de n jour(s)

Si l'option est activée, les événements sont supprimés de la base de données d'événements après un certain nombre de jours ; les valeurs autorisées sont : 1 à 90 jours. Cette option est définie par défaut sur une valeur de 30 jours.

Pas de limitation

Si l'option est activée, la taille de la base de données d'événements n'est pas limitée. Toutefois, 20 000 entrées au maximum sont affichées sur l'interface du programme sous Événements.

9.8.7 Rapports

Limiter les rapports

Limiter le nombre maximum à n unités

Si cette option est activée, le nombre maximum de rapports peut être limité ; les valeurs autorisées sont : 1 à 300. Si le nombre indiqué est dépassé, les rapports les plus anciens sont supprimés.

Supprimer tous les rapports de plus de n jour(s)

Si cette option est activée, les rapports sont supprimés automatiquement après un certain nombre de jours ; valeurs autorisées : 1 à 90 jours. Cette option est définie par défaut sur une valeur de 30 jours.

Pas de limitation

Si cette option est activée, le nombre de rapports n'est pas limité.

9.8.8 Répertoires

Chemin temporaire

Utiliser le paramètre du système

Si cette option est activée, les paramètres du système sont utilisés pour le traitement des fichiers temporaires.

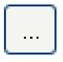
> **Remarque**
> Pour savoir où votre système enregistre les fichiers temporaires, sur Windows XP par exemple, allez sous : **Démarrer > Panneau de configuration > Performances et maintenance > Système >** onglet « **Avancé** » > bouton « **Variables d'environnement** ». Les variables temporaires (`TEMP`, `TMP`) pour l'utilisateur connecté et pour les variables du système (`TEMP`, `TMP`) sont visibles ici avec leurs valeurs respectives.

Utiliser le répertoire suivant

Si l'option est activée, c'est le chemin indiqué dans le champ de saisie qui est utilisé.

Champ de saisie

Entrez dans ce champ de saisie le chemin sous lequel le programme doit enregistrer les fichiers temporaires.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le chemin temporaire souhaité.

Par défaut

Ce bouton restaure le répertoire prédéfini pour le chemin temporaire.

9.8.9 Avertissement sonore

En cas de détection d'un virus ou d'un logiciel malveillant par le scanner ou la protection temps réel, un signal sonore d'avertissement retentit dans le mode d'action interactif. Vous pouvez désactiver ou activer le signal sonore d'avertissement, ou sélectionner un autre fichier WAVE comme signal sonore d'avertissement.

> **Remarque**
> Le mode d'action du scanner se règle dans la configuration sous Sécurité PC > Scanner > Recherche > Action si résultat positif. Le mode d'action de la protection temps réel se règle dans la configuration sous Sécurité PC > Protection temps réel > Recherche > Action si résultat positif.

Pas d'avertissement

Si l'option est activée, aucun avertissement sonore ne se produit lors de la détection d'un virus par le scanner ou la protection temps réel.

Diffuser par le haut-parleur du PC (uniquement en mode interactif)

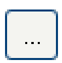
Si l'option est activée, un avertissement sonore se produit à l'aide d'un signal sonore d'avertissement par défaut, lors de la détection d'un virus par le scanner ou la protection temps réel. Le signal sonore d'avertissement est diffusé par le haut-parleur interne du PC.

Utiliser le fichier WAVE suivant (uniquement en mode interactif)

Si l'option est activée, un avertissement sonore se produit à l'aide du fichier WAVE sélectionné, en cas de détection d'un virus par le scanner ou la protection temps réel. Le fichier WAVE sélectionné est diffusé par un haut-parleur externe raccordé.

Fichier WAVE

Dans ce champ de saisie, vous pouvez saisir le nom et le chemin correspondant d'un fichier audio de votre choix. Le signal sonore d'avertissement par défaut du programme est indiqué comme préréglage.



Ce bouton ouvre une fenêtre dans laquelle vous avez la possibilité de sélectionner le fichier souhaité à l'aide de l'explorateur de fichiers.

Test

Ce bouton sert à tester le fichier WAVE sélectionné.

9.8.10 Avertissements

Pour certains événements, votre produit Avira affiche des notifications sur le Bureau (slide-up), pour vous informer de dangers et de la réussite ou de l'échec de l'exécution de

programmes, p. ex. l'exécution d'une mise à jour. Sous **Avertissements**, vous pouvez activer ou désactiver la notification de certains événements.

En cas de notifications affichées sur le Bureau, vous avez la possibilité de désactiver directement la notification dans le slide-up. Vous pouvez annuler la désactivation de la notification dans la fenêtre de configuration **Avertissements**.

Mise à jour

Avertissement si la dernière mise à jour date de plus de n jour(s)

Dans ce champ, vous pouvez saisir le nombre de jours maximum qui doit s'être écoulé depuis la dernière mise à jour. Si cette période est dépassée, une icône rouge s'affiche dans le Control Center sous État pour l'état de mise à jour.

Afficher un avertissement si le fichier de définitions des virus est obsolète

Si l'option est activée, vous recevez un message d'avertissement en cas de fichier de définitions des virus obsolète. À l'aide de l'option « Avertissement si la dernière mise à jour date de plus de n jour(s) », vous pouvez configurer l'intervalle avant l'avertissement.

Avertissements / remarques dans les situations suivantes

Une connexion par modem est utilisée

Si l'option est activée, une notification s'affiche sur le Bureau pour vous avertir lorsqu'un programme de numérotation établit sur votre ordinateur une connexion par téléphone ou par réseau RNIS. Le programme de numérotation risque d'être un numéroteur inconnu et indésirable qui établit une connexion payante. (Voir Virus et autres > Programmes de numérotation payants)

Les fichiers ont été actualisés avec succès

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a réussi et que les fichiers ont été actualisés.

Échec de la mise à jour

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a échoué : la connexion au serveur de téléchargement n'a pas pu être établie ou les fichiers de mise à jour n'ont pas pu être installés.

Aucune mise à jour n'est nécessaire

Si l'option est activée, une notification s'affiche sur le Bureau lorsqu'une mise à jour a été lancée sans qu'il soit toutefois nécessaire d'installer des fichiers car votre programme est à jour.

10. Icône de la barre d'état

L'icône de barre d'état dans la zone de notification de la barre des tâches affiche l'état de la Protection temps réel.

Icône	Description
	La protection temps réel Avira est activée
	La protection temps réel Avira est désactivée

Entrées dans le menu contextuel

- **Activer la protection temps réel** : active ou désactive la protection temps réel Avira.
- **Activer la protection e-mail** : active ou désactive la protection e-mail Avira.
- **Activer la protection Web** : active ou désactive la protection Web Avira.
  - **Activer Pare-feu Windows** : active ou désactive Pare-feu Windows (cette fonction est disponible à partir de Windows 8 seulement).
- **Démarrer Avira Antivirus Suite** : ouvre le Control Center.
- Configurer **Avira Antivirus Suite** : ouvre la configuration.
- **Mes messages** : ouvre un message-bannière avec les derniers messages concernant votre produit Avira.
- **Mes paramètres de communication** : ouvre le centre d'abonnement pour les notifications produits
- **Démarrer mise à jour** : démarre une mise à jour.
- **Aide** : ouvre l'aide en ligne.
- **À propos de Avira Antivirus Suite** :
  ouvre une boîte de dialogue avec des informations sur votre produit Avira : informations sur le produit, la version, la licence.
- **Avira sur Internet** :
  ouvre le portail Web Avira sur Internet. Un accès Internet est nécessaire.

11. Notifications produits

11.1.1 Centre d'abonnement pour les notifications produits

En cliquant sur **Mes paramètres de communication** dans le menu contextuel de l'icône de barre d'état Avira ou en cliquant sur l'icône de **Configuration** dans le message-bannière **Mes messages**, vous accédez au *centre d'abonnement pour les notifications produits* sur notre page Web.

- Vous avez la possibilité de contrôler le flux d'informations des notifications produits en cliquant sur les boutons **Activé/Désactivé** correspondants.
- Cliquez ensuite sur **Mettre le profil à jour** pour enregistrer votre profil de notification.
  - ↳ Un message s'affiche, vous indiquant que votre profil de notification a été correctement mis à jour.

Contactez-nous en ligne en cliquant sur l'un des liens.

11.1.2 Messages actuels

Le message-bannière *Mes messages* sert d'interface de communication. Il vous présente les dernières évolutions de la Sécurité Internet, les actualités des produits Avira (mises à jour, mises à niveau et notifications de licence) et des informations sur les virus.

S'il n'y a pas de nouveau message, vous recevez la notification *Aucun nouveau message*. Cliquez sur **OK** pour fermer le message-bannière.

En cas de nouveaux messages, vous disposez des possibilités suivantes :

- Cliquez sur **Me rappeler plus tard** pour lire les derniers messages ultérieurement.
- Cliquez sur **+ plus** pour lire les détails du message.
  - ↳ Selon le type de message, vous êtes dirigé vers notre site Internet ou vous obtenez des informations dans une nouvelle fenêtre.
- Cliquez sur la petite croix **x** pour fermer les différents messages.
- Cliquez sur l'icône de **Configuration** dans l'en-tête du message-bannière pour enregistrer votre profil de notification personnalisé.

12. FireWall

Avira Antivirus Suite vous permet de surveiller et de réguler le trafic de données entrantes et sortantes en fonction des paramètres de votre ordinateur :

- Pare-feu Windows

Avira FireWall n'est plus compris dans Avira Antivirus Suite à partir de Windows 7. À la place, vous avez la possibilité de régler Pare-feu Windows à l'aide du centre de contrôle et de configuration.

12.1 Pare-feu Windows

Avira FireWall n'est plus compris dans Avira Antivirus Suite à partir de Windows 7. À la place, vous avez la possibilité de régler Pare-feu Windows à l'aide du centre de contrôle et de configuration. Pour paramétrer Pare-feu Windows, vous disposez des options suivantes :

Activation de Pare-feu Windows dans le Control Center

Vous pouvez activer ou désactiver Pare-feu Windows en cliquant sur le bouton **ON/OFF** de l'option *FireWall* sous **État > Sécurité Internet**.

Contrôle de l'état du Pare-feu Windows dans le Control Center

Vous pouvez contrôler l'état de Pare-feu Windows sous la rubrique **SÉCURITÉ INTERNET > FireWall** et restaurer les paramètres recommandés en cliquant sur le bouton **Résoudre le problème**.

13. Mises à jour

13.1 Mises à jour

L'efficacité d'un logiciel antivirus dépend de la mise à jour du programme, et tout particulièrement de celle du fichier de définitions des virus et du moteur de recherche. Le composant Updater est intégré dans votre produit Avira pour l'exécution des mises à jour. Il garantit que votre produit Avira fonctionne toujours au niveau le plus récent et qu'il est en mesure de détecter les nouveaux virus apparaissant chaque jour. L'Updater met à jour les composants suivants :

- Fichier de définitions des virus :

  Le fichier de définitions des virus contient le modèle de détection des programmes malveillants, que votre produit Avira utilise lors de la recherche de virus et de logiciels malveillants, ainsi que lors de la réparation des objets infectés.

- Moteur de recherche :

  Le moteur de recherche contient les méthodes à l'aide desquelles votre produit Avira recherche des virus et logiciels malveillants.

- Fichiers de programme (mise à jour du produit) :

  Les paquets pour les mises à jour du produit offrent des fonctions supplémentaires pour les différents composants du programme.

Lors de l'exécution d'une mise à jour, on vérifie que le fichier de définitions des virus, le moteur de recherche et les fichiers de programme sont actuels, et ils sont mis à jour si nécessaire. Après une mise à jour du produit, il peut être nécessaire d'effectuer un redémarrage de votre ordinateur. S'il ne s'effectue qu'une mise à jour du fichier de définitions des virus et du moteur de recherche, il n'est pas nécessaire de redémarrer votre ordinateur.

Si un redémarrage est nécessaire après une mise à jour du produit, vous pouvez décider si vous souhaitez poursuivre la mise à jour ou si vous souhaitez recevoir un rappel ultérieur. Si vous décidez de poursuivre la mise à jour, vous devez tout de même déterminer le moment où l'ordinateur doit être redémarré.

Si vous désirez exécuter la mise à jour du produit à une date ultérieure, le fichier de définitions des virus et le moteur de recherche sont tout de même actualisés, mais pas les fichiers de programme.

> **Remarque**
> La mise à jour du produit n'est pas achevée tant que l'ordinateur n'a pas été redémarré.

Remarque
Pour des raisons de sécurité, l'Updater contrôle si le fichier *hôte* Windows de votre ordinateur a été modifié, si l'URL de mise à jour a par ex. été manipulée par un logiciel malveillant, et redirige l'Updater vers des pages de téléchargement indésirables. Si le fichier hôte Windows a été manipulé, l'opération est visible dans le fichier rapport de l'Updater.

Une mise à jour est exécutée automatiquement dans l'intervalle suivant : 2 heures.

Dans le Control Center, sous **Planificateur**, vous pouvez configurer d'autres tâches de mise à jour qui seront exécutées par l'Updater aux intervalles indiqués. Vous avez aussi la possibilité de démarrer manuellement une mise à jour :

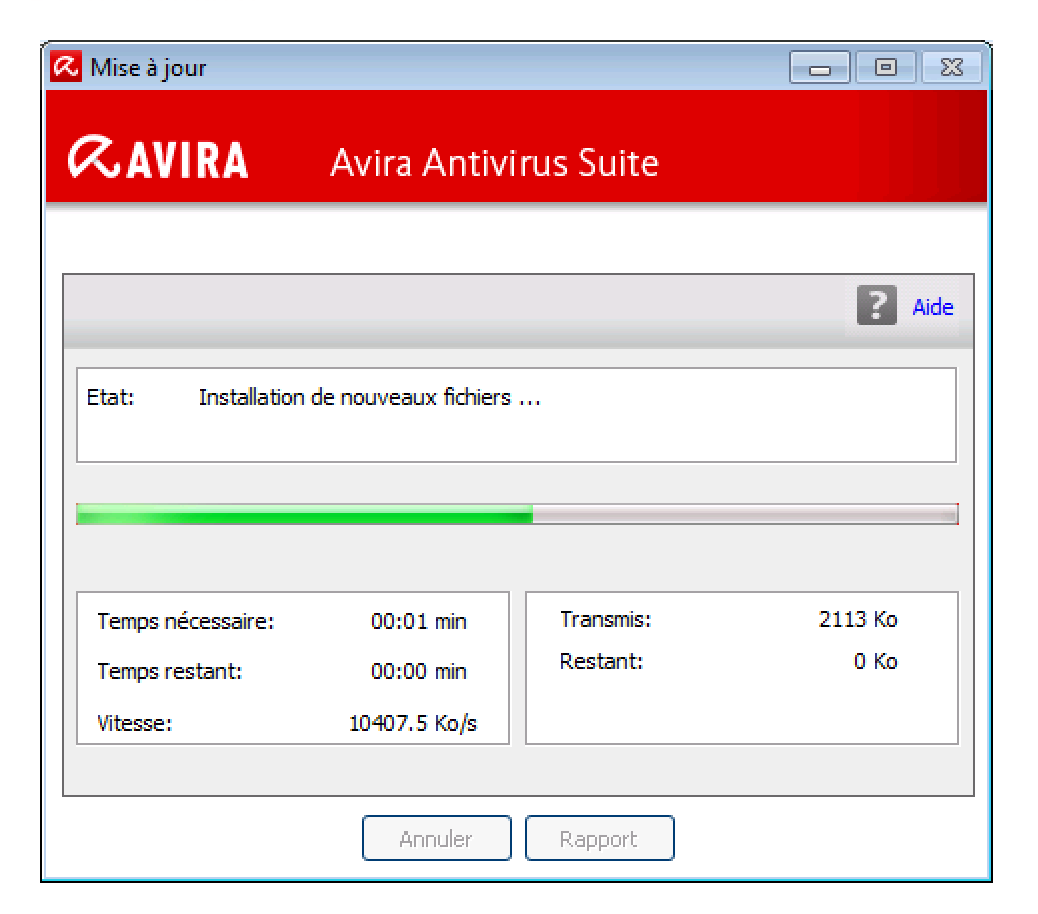
- Dans le Control Center : dans le menu **Mise à jour** et sous la rubrique **État**
- Via le menu contextuel de l'icône de la barre d'état

Vous pouvez obtenir des mises à jour à partir d'Internet, via un serveur Web du fabricant. Par défaut, la connexion réseau existante est utilisée comme connexion aux serveurs de téléchargement Avira. Vous pouvez adapter ce paramètre par défaut sous Configuration > Mise à jour.

13.2 Updater

La fenêtre de l'Updater s'ouvre après le démarrage d'une mise à jour.





Remarque
Dans le cas de tâches de mise à jour créées dans le planificateur, vous pouvez paramétrer le **mode d'affichage** pour la fenêtre de la mise à jour : vous pouvez sélectionner les modes **Invisible**, **Réduit** ou **Agrandi**.

Remarque
Si vous travaillez avec un programme en mode plein écran (par ex. jeux) et que l'Updater se trouve en mode d'affichage agrandi ou réduit, il bascule brièvement sur le Bureau. Pour empêcher ceci, vous pouvez également démarrer l'Updater en mode d'affichage invisible. Ainsi, vous ne serez plus prévenu d'une mise à jour par la fenêtre de mise à jour.

État : indique la procédure actuelle de l'Updater.

Temps écoulé : temps écoulé depuis le démarrage de la procédure de téléchargement.

Temps restant : temps restant jusqu'à la fin de la procédure de téléchargement.

Vitesse : vitesse à laquelle les fichiers sont téléchargés.

Transférés : octets déjà téléchargés.



Restants : octets qui n'ont pas encore été téléchargés.

Boutons et liens

Bouton / Lien	Description
Aide	Ce bouton ou lien vous permet d'ouvrir cette page de l'aide en ligne.
Réduire	La fenêtre d'affichage de l'Updater s'affiche de manière réduite.
Agrandir	La fenêtre d'affichage de l'Updater est restaurée à sa taille d'origine.
Annuler	La procédure de mise à jour est interrompue. L'Updater est fermé.
Quitter	La procédure de mise à jour est terminée. La fenêtre d'affichage se ferme.
Rapport	Le fichier rapport de la mise à jour s'affiche.

14. Résolution des problèmes, astuces

Dans ce chapitre, vous trouverez des informations importantes pour le dépannage, ainsi que d'autres astuces pour utiliser votre produit Avira.

- voir chapitre Aide en cas de problème
- voir chapitre Commandes clavier
- voir chapitre Centre de sécurité Windows (pour Windows XP) ou Centre de maintenance Windows (à partir de Windows 7)

14.1 Aide en cas de problème

Vous trouverez ici des informations sur les causes et solutions de problèmes possibles.

- Le message d'erreur *Le fichier de licence ne s'ouvre pas* s'affiche.
- Le message d'erreur *L'établissement de la connexion a échoué lors du téléchargement du fichier...* apparaît lorsque vous essayez de démarrer une mise à jour.
- Les virus et logiciels malveillants ne peuvent pas être déplacés ou supprimés.
- L'icône de la barre d'état indique un état de désactivation.
- L'ordinateur devient très lent quand j'enregistre des données.
- Mon pare-feu signale la protection temps réel Avira et la protection e-mail Avira dès qu'elles sont actives
- La protection e-mail Avira ne fonctionne pas.
- Un e-mail envoyé via une connexion TLS a été bloqué par la protection e-mail.
- Le chat Internet ne fonctionne pas : les messages du chat ne s'affichent pas.

Le message d'erreur *Le fichier de licence ne s'ouvre pas* s'affiche.

Cause : le fichier est codé.

- Pour activer la licence, il n'est pas nécessaire d'ouvrir le fichier mais il faut l'enregistrer dans le répertoire de programmes.

Le message d'erreur *L'établissement de la connexion a échoué lors du téléchargement du fichier...* apparaît lorsque vous essayez de démarrer une mise à jour.

Cause : votre connexion Internet est inactive. C'est pourquoi aucune connexion au serveur Web sur Internet ne peut être établie.

- Testez le fonctionnement d'autres services Internet comme WWW ou le courrier électronique. S'ils ne fonctionnent pas, restaurez la connexion Internet.

Cause : le serveur proxy n'est pas accessible.



- Contrôlez si les données de connexion au serveur proxy ont changé et adaptez votre configuration si nécessaire.

Cause : le fichier *update.exe* n'est pas intégralement autorisé par votre pare-feu personnel.

- Assurez-vous d'autoriser complètement le fichier *update.exe* auprès de votre pare-feu.

Sinon :

- Vérifiez dans la configuration sous Sécurité PC > Mise à jour.

Les virus et logiciels malveillants ne peuvent pas être déplacés ou supprimés.

Cause : le fichier a été chargé par Windows et se trouve à l'état activé.

- Actualisez votre produit Avira.
- Si vous utilisez le système d'exploitation Windows XP, désactivez la restauration du système.
- Démarrez l'ordinateur en mode sécurisé.
- Ouvrez la configuration de votre produit Avira.
- Sélectionnez **Scanner > Recherche**, dans le champ *Fichier* sélectionnez l'option **Tous les fichiers** et confirmez la fenêtre avec **OK**.
- Démarrez une recherche sur tous les lecteurs locaux.
- Démarrez l'ordinateur en mode normal.
- Effectuez une recherche en mode normal.
- Si aucun autre virus ni logiciel malveillant n'est détecté, activez la restauration du système si elle est disponible et doit être utilisée.

L'icône de la barre d'état indique un état de désactivation.

Cause : la protection temps réel a été désactivée.

- Dans le Control Center, cliquez sur le point **État** et dans la zone *Sécurité PC*, activez la **Protection temps réel**.

- - OU -

- Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état. Le menu contextuel s'ouvre. Cliquez sur **Activer la protection temps réel**.

Cause : la protection temps réel est bloquée par un pare-feu.

- Dans la configuration de votre pare-feu, définissez une autorisation générale pour la protection temps réel Avira. La protection temps réel Avira fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie. Il en va de même pour la protection e-mail Avira.

Sinon :

- Vérifiez le type de démarrage du service Protection temps réel Avira. Le cas échéant, activez le service : dans la barre de démarrage, sélectionnez **Démarrer > Panneau de configuration**. Lancez la fenêtre de configuration **Services** par double clic (sous Windows XP, vous trouvez l'applet Services dans le sous-dossier *Outils d'administration*). Recherchez l'entrée *Protection temps réel Avira*. Comme type de démarrage, vous devez sélectionner `Automatique` et comme statut `Démarré`. Le cas échéant, démarrez le service manuellement en sélectionnant la ligne correspondante et le bouton **Démarrer**. Si un message d'erreur s'affiche, contrôlez l'affichage de l'événement.

L'ordinateur devient très lent quand j'enregistre des données.

Cause : la protection temps réel Avira parcourt tous les fichiers que la sauvegarde des données traite lors du processus de sauvegarde.

- Dans la configuration , sélectionnez **Protection temps réel > Recherche > Exceptions** et saisissez le nom du processus du logiciel de sauvegarde.

Mon pare-feu signale la protection temps réel Avira et la protection e-mail Avira, dès qu'elles sont activées.

Cause : la communication de la protection temps réel Avira et de la protection e-mail Avira s'effectue via le protocole Internet TCP/IP. Un pare-feu surveille toutes les connexions via ce protocole.

- Définissez une autorisation générale pour la protection temps réel et la protection e-mail Avira. La protection temps réel Avira fonctionne uniquement avec l'adresse 127.0.0.1 (localhost). Aucune connexion à Internet n'est établie. Il en va de même pour la protection e-mail Avira.

La protection e-mail Avira ne fonctionne pas.

✓ Contrôlez la fonctionnalité de la protection e-mail Avira à l'aide des checklists suivantes, si des problèmes se produisent avec la protection e-mail Avira.

Checklists

✓ Vérifiez si votre client de messagerie se connecte au serveur par Kerberos, APOP ou RPA. Ces méthodes d'authentification ne sont pas prises en charge actuellement.

✓ Contrôlez si votre client de messagerie se connecte au serveur par SSL (également souvent appelé TLS - Transport Layer Security). La protection e-mail Avira ne prend pas en charge SSL et arrête donc les connexions codées SSL. Si vous voulez utiliser les connexions codées SSL sans la protection e-mail Avira, vous devez utiliser pour la connexion un autre port que les ports surveillés par la protection e-mail. Vous pouvez configurer les ports surveillés par la protection e-mail dans la configuration sous **Protection e-mail > Recherche**.

✓ La protection e-mail Avira (service) est-elle active ? Le cas échéant, activez le service : dans la barre de démarrage, sélectionnez **Démarrer > Panneau de configuration**. Lancez la fenêtre de configuration **Services** par double clic (sous

Windows XP, vous trouvez l'applet Services dans le sous-dossier *Outils d'administration*). Recherchez l'entrée *Protection e-mail Avira*. Comme type de démarrage, vous devez sélectionner `Automatique` et comme statut `Démarré`. Le cas échéant, démarrez le service manuellement en sélectionnant la ligne correspondante et le bouton **Démarrer**. Si un message d'erreur s'affiche, contrôlez l'*Affichage de l'événement*. Si cela ne résout pas le problème, désinstallez complètement le produit Avira via **Démarrer > Panneau de configuration > Programmes**, redémarrez l'ordinateur et réinstallez ensuite votre produit Avira.

Généralités

- Les connexions POP3 codées via SSL (Secure Sockets Layer) (souvent appelées TLS (Transport Layer Security)) ne peuvent pas être protégées actuellement et sont ignorées.
- L'authentification lors de la connexion au serveur de messagerie électronique est actuellement prise en charge uniquement via des mots de passe. « Kerberos » et « RPA » ne sont actuellement pas pris en charge.
- Votre produit Avira ne contrôle pas l'absence de virus et de programmes indésirables dans les e-mails lors de leur expédition.

> **Remarque**
> Nous vous recommandons d'effectuer régulièrement des mises à jour Microsoft pour combler d'éventuelles lacunes de sécurité.

Un e-mail envoyé via une connexion TLS a été bloqué par la protection e-mail.

Cause : Transport Layer Security (TLS : protocole de cryptage pour la transmission de données par Internet) n'est actuellement pas pris en charge par la protection e-mail. Vous disposez des possibilités suivantes pour envoyer l'e-mail :

- Utilisez un autre port que le port 25 utilisé par SMTP. Vous contournerez ainsi la surveillance de la protection e-mail.
- Renoncez à utiliser la connexion cryptée TLS et désactivez la prise en charge TLS de votre client de messagerie.
- Désactivez (provisoirement) la surveillance des e-mails sortants par la protection e-mail dans la configuration sous **Protection e-mail > Recherche**.

Le chat Internet ne fonctionne pas : les messages du chat ne s'affichent pas.

Ce phénomène peut se produire dans les chats basés sur le protocole HTTP avec 'transfer-encoding: chunked'.

Cause : la protection Web contrôle d'abord intégralement l'absence de virus et de programmes indésirables sur les données envoyées avant de charger celles-ci dans le navigateur Internet. Lors du transfert de données avec 'transfer-encoding: chunked', la



protection Web ne peut pas déterminer la longueur des messages ou la quantité de données.

- Indiquez l'URL du chat Internet comme exception dans la configuration (voir configuration : Protection Web > Recherche > Exceptions).

14.2 Commandes clavier

Les commandes clavier - aussi appelées raccourcis clavier - permettent de naviguer dans le programme, d'accéder à divers modules et de démarrer des actions rapidement.

Ci-après, vous trouverez un aperçu des commandes clavier disponibles. Le chapitre correspondant de l'Aide vous donne plus d'informations sur les fonctionnalités et la disponibilité de ces commandes.

14.2.1 Dans les boîtes de dialogue

Commande clavier	Description
Ctrl + Tab **Ctrl + PgDn**	Navigation dans le Control Center Passer à la rubrique suivante.
Ctrl + Maj + Tab **Ctrl + PgDn**	Navigation dans le Control Center Passer à la rubrique précédente.
←↑→↓	Navigation dans les rubriques de configuration Faites d'abord glisser la souris sur la rubrique de configuration que vous souhaitez consulter. Naviguer entre les options dans un champ de liste déroulante sélectionné ou entre les options dans un groupe d'options.
Tab	Passer à l'option suivante ou au groupe d'options suivant.
Maj + Tab	Passer à l'option précédente ou au groupe d'options précédent.
Touche espace	Activation et désactivation d'une case à cocher lorsque l'option active est une case à cocher.

Alt + lettre soulignée	Sélectionner une option ou exécuter une commande.
Alt + ↓ **F4**	Ouvrir le champ de liste déroulante sélectionné.
Échap	Fermer le champ de liste déroulante sélectionné. Annuler la commande et fermer la boîte de dialogue.
Touche Entrée	Exécuter la commande pour l'option active ou le bouton actif.

14.2.2 Dans l'Aide

Commande clavier	Description
Alt + touche espace	Afficher le menu système.
Alt + Tab	Naviguer entre l'Aide et les autres fenêtres ouvertes.
Alt + F4	Fermer l'Aide.
Maj + F10	Afficher les menus contextuels de l'Aide.
Ctrl + Tab	Passer à la rubrique suivante dans la fenêtre de navigation.
Ctrl + Maj + Tab	Passer à la rubrique précédente dans la fenêtre de navigation.
PgUp	Passer au thème situé au-dessus du thème actuel dans le sommaire, l'index ou la liste des résultats de recherche.
PgDn	Passer au thème situé en dessous du thème actuel dans le sommaire, l'index ou la liste des résultats de recherche.

PgUp **PgDn**	Parcourir un thème.

14.2.3 Dans le Control Center

Généralités

Commande clavier	Description
F1	Afficher l'Aide
Alt + F4	Fermer le Control Center
F5	Actualiser la vue
F8	Ouvrir la configuration
F9	Démarrer mise à jour

Rubrique **Scanner**

Commande clavier	Description
F2	Renommer le profil sélectionné
F3	Démarrer la recherche avec le profil choisi
F4	Créer un raccourci sur le Bureau pour le profil sélectionné
Ins	Créer un nouveau profil
Suppr	Supprimer le profil sélectionné

Rubrique **Quarantaine**

Commande clavier	Description
F2	Contrôler à nouveau l'objet
F3	Restaurer l'objet
F4	Envoyer l'objet
F6	Restaurer l'objet à l'emplacement...
Entrée	Propriétés
Ins	Ajouter le fichier
Suppr	Supprimer l'objet

Rubrique **Planificateur**

Commande clavier	Description
F2	Modifier la tâche
Entrée	Propriétés
Ins	Ajouter une nouvelle tâche
Suppr	Supprimer la tâche

Rubrique **Rapports**

Commande clavier	Description
F3	Afficher le fichier rapport
F4	Imprimer le fichier rapport
Entrée	Afficher le rapport
Suppr	Supprimer le(s) rapport(s)

Rubrique **Événements**

Commande clavier	Description
F3	Exporter le(s) événement(s)
Entrée	Afficher l'événement
Suppr	Supprimer le(s) événement(s)

14.3 Centre de sécurité Windows

- De Windows XP Service Pack 2 -

14.3.1 Généralités

Le Centre de sécurité Windows vérifie l'état d'un ordinateur concernant les aspects importants de la sécurité.

Si un problème est constaté sur l'un de ces points importants (par exemple, un programme antivirus obsolète), le Centre de sécurité envoie un avertissement et émet des recommandations pour mieux protéger l'ordinateur.

14.3.2 Le Centre de sécurité Windows et votre produit Avira

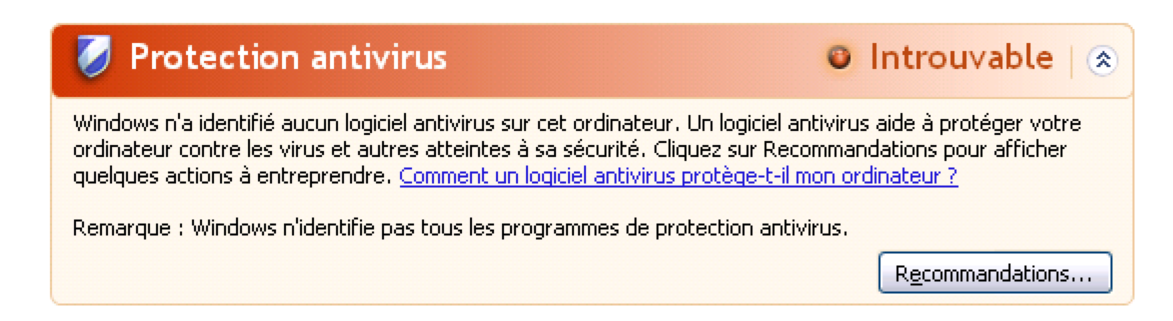
Logiciel antivirus / Protection contre les logiciels nuisibles

Vous pouvez recevoir les remarques suivantes du Centre de sécurité Windows, concernant votre protection antivirus :

- Protection antivirus NON TROUVÉE
- Protection antivirus EXPIRÉE
- Protection antivirus ACTIVÉE
- Protection antivirus DÉSACTIVÉE
- Protection antivirus NON SURVEILLÉE

Protection antivirus NON TROUVÉE

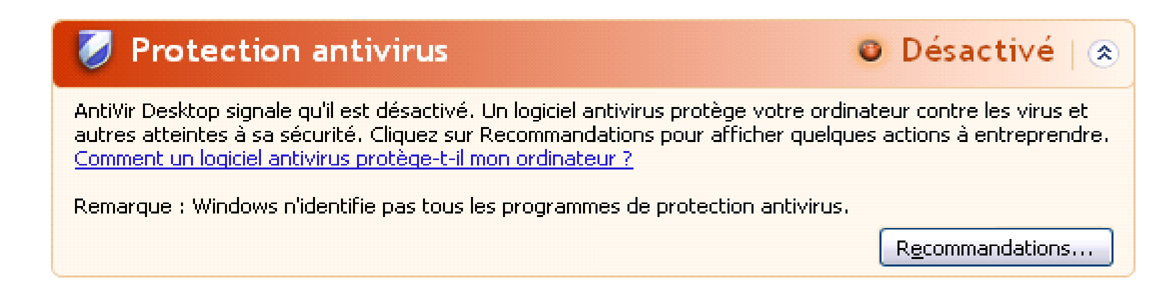
Cette notification du Centre de sécurité Windows apparaît si celui-ci n'a trouvé aucun logiciel antivirus sur votre ordinateur.



> **Remarque**
> Installez le produit Avira sur votre ordinateur pour le protéger des virus et autres programmes indésirables.

Protection antivirus EXPIRÉE

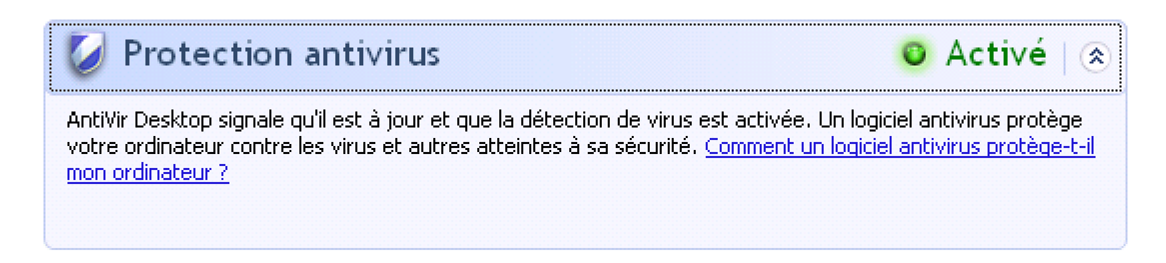
Si Windows XP Service Pack 2 est déjà installé sur votre ordinateur, puis que vous installez votre produit Avira, ou si vous installez Windows XP Service Pack 2 sur un système accueillant déjà le produit Avira, vous recevez le message suivant :



> **Remarque**
> Pour que le Centre de sécurité Windows identifie votre produit Avira comme mis à jour, vous devez obligatoirement effectuer une mise à jour après l'installation. Vous actualisez votre système en exécutant une Mise à jour.

Protection antivirus ACTIVÉE

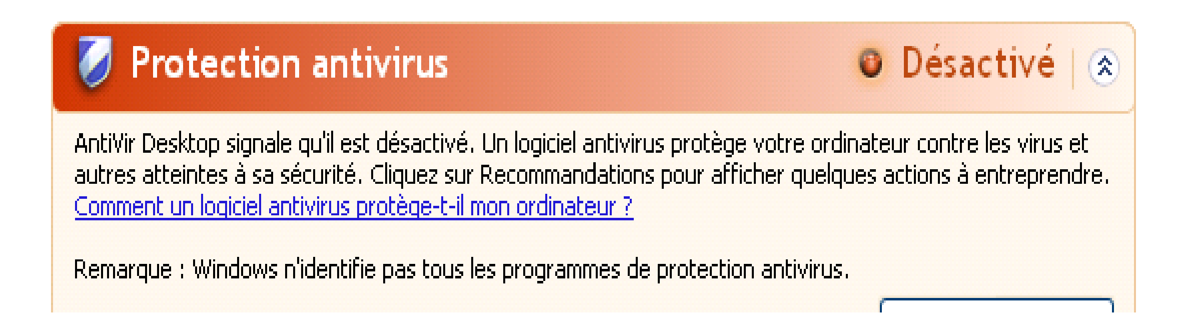
Après l'installation de votre produit Avira et une mise à jour effectuée par la suite, vous recevez le message suivant :



Votre produit Avira est maintenant à jour et la protection temps réel Avira est activée.

Protection antivirus DÉSACTIVÉE

Vous recevez le message suivant si vous désactivez la protection temps réel Avira ou si vous arrêtez le service Protection temps réel.

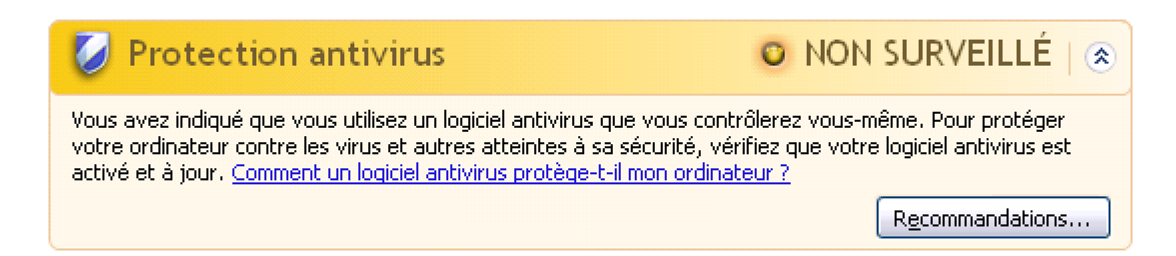


> **Remarque**
> Vous pouvez activer ou désactiver la protection temps réel Avira dans la rubrique État du **Control Center**. Vous voyez en outre que la protection temps réel Avira est activée lorsque le parapluie rouge est ouvert dans la barre des tâches.

Protection antivirus NON SURVEILLÉE

Si vous recevez le message suivant du Centre de sécurité Windows, c'est que vous avez choisi de surveiller vous-même votre logiciel antivirus.





Remarque
Le Centre de sécurité Windows est pris en charge par votre produit Avira. Vous pouvez activer cette option à tout moment via le bouton **Recommandations...**.

Remarque
Même si vous avez installé Windows XP Service Pack 2, il vous faut toujours une protection antivirus. Bien que Windows surveille votre logiciel antivirus, il ne dispose d'aucune fonction antivirus. Aussi, sans protection antivirus supplémentaire, vous ne seriez pas protégé des virus et autres logiciels malveillants !

14.4 Centre de maintenance Windows

- Windows 7 et Windows 8 -

14.4.1 Généralités

Remarque :
Á partir de Windows 7, le **Centre de sécurité Windows** a été renommé **Centre de maintenance Windows**. Dans cette section du programme, vous trouvez l'état de toutes les options de sécurité.

Le Centre de maintenance Windows vérifie l'état d'un ordinateur concernant les aspects importants de la sécurité. Vous pouvez accéder directement au Centre de maintenance en cliquant sur le petit drapeau de la barre des tâches ou sous **Panneau de configuration > Centre de maintenance**.

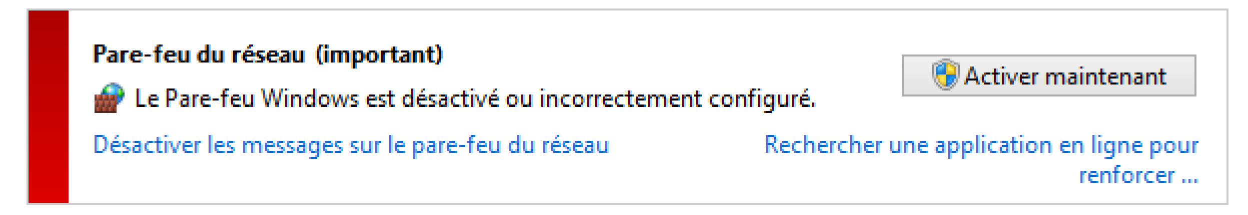
Si un problème est constaté sur l'un de ces points importants (par ex. un programme antivirus dépassé), le Centre de maintenance envoie un avertissement et émet des recommandations pour mieux protéger l'ordinateur. En d'autres termes, si tout fonctionne bien, vous ne recevez aucun message du Centre de maintenance. Cependant, il est possible de surveiller l'état de la sécurité de l'ordinateur dans le **Centre de maintenance** sous la rubrique **Sécurité**.
Vous avez également la possibilité de gérer et de sélectionner les logiciels que vous avez installés (par ex. *Afficher les programmes anti-espion installés*).



Vous pouvez désactiver les messages d'avertissement sous **Centre de maintenance > Modifier les paramètres**(par ex.*Désactiver les messages de sécurité pour la protection contre les logiciels espions et logiciels malveillants*).

14.4.2 Le Centre de maintenance Windows et votre produit Avira

Pare-feu Windows est désactivé ou n'est pas configuré correctement



- **Pare-feu Windows**
- À partir de Windows 7 vous avez la possibilité de régler Pare-feu Windows à l'aide du centre de contrôle et de configuration.

Protection antivirus

Vous pouvez recevoir les remarques suivantes du Centre de maintenance Windows, concernant votre protection antivirus :

- Avira Desktop indique être à jour et que la détection des virus est activée
- Avira Desktop indique qu'il est désactivé
- Avira Desktop indique qu'il est périmé
- Windows n'a pas trouvé de logiciel antivirus sur cet ordinateur
- Avira Desktop ne protège plus votre PC

Avira Desktop indique être à jour et que la détection des virus est activée

Après l'installation de votre produit Avira et après une mise à jour effectuée ensuite, vous ne recevez tout d'abord aucun message du Centre de maintenance Windows. Cependant, sous **Centre de maintenance > Sécurité**, vous pouvez trouver les indications suivantes : *« Avira Desktop » indique être à jour et que la détection de virus est activée*. Cela signifie que votre produit Avira est maintenant à jour et que la protection temps réel est activée.

Avira Desktop indique qu'il est désactivé

Vous recevez le message suivant si vous désactivez la protection temps réel Avira ou si vous arrêtez le service Protection temps réel.

Protection antivirus (important)	Activer maintenant
Avira Desktop indique qu'il est désactivé.	
Désactiver les messages concernant la protection antivirus	Télécharger un autre programme antivirus

Remarque
Vous pouvez activer ou désactiver la **protection temps réel Avira** sous la rubrique **État** de l'**Avira Control Center**. Vous voyez en outre que la **protection temps réel Avira** est activée lorsque le parapluie rouge est ouvert dans votre barre des tâches. Il est également possible d'activer les différents composants Avira en cliquant sur *Activer maintenant* du Centre de maintenance. Si vous obtenez un message où vous devez donner votre accord pour lancer le programme Avira, cliquez sur *Autoriser*, et la protection temps réel est activée.

Avira Desktop indique qu'il est périmé

Si vous venez d'installer Avira, ou si pour une raison quelconque le fichier de définitions des virus, le moteur de recherche ou les fichiers de programme de votre produit Avira n'ont pas été mis à jour automatiquement (par ex. si vous mettez à jour votre système d'exploitation, sur lequel vous avez déjà installé votre produit Avira, pour passer d'une ancienne version de Windows à une nouvelle), le message suivant s'affiche :

Protection antivirus (important)	Mettre à jour maintenant
Avira Desktop indique qu'il est périmé.	
Désactiver les messages concernant la protection antivirus	Télécharger un autre programme antivirus

Remarque
Pour que le Centre de maintenance identifie votre produit Avira comme mis à jour, vous devez obligatoirement effectuer une mise à jour après l'installation. Vous actualisez votre système en exécutant une Mise à jour.

Windows n'a pas trouvé de logiciel antivirus sur cet ordinateur

Cette notification du Centre de maintenance Windows apparaît si le Centre de maintenance Windows n'a trouvé aucun logiciel antivirus sur votre ordinateur.

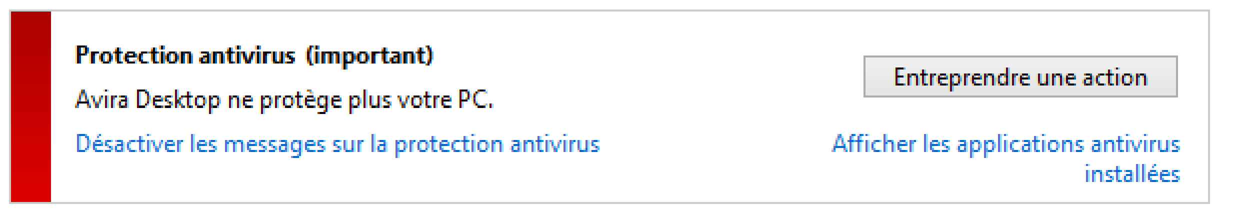
Protection antivirus (important)	Télécharger un programme
Windows n'a pas trouvé de logiciel antivirus sur cet ordinateur.	
Désactiver les messages concernant la protection antivirus	

Remarque
Veuillez noter que cette option n'est pas disponible sous Windows 8. À partir de ce système d'exploitation, Windows Defender est la protection antivirus Microsoft par défaut.

Remarque
Installez votre produit Avira sur votre ordinateur pour le protéger des virus et autres programmes indésirables !

Avira Desktop ne protège plus votre PC

Cette information du Centre de maintenance Windows apparaît lorsque la licence de votre produit Avira a expiré.
Si vous cliquez sur le bouton **Entreprendre une action**, vous serez redirigé vers le site Web d'Avira, où vous pourrez obtenir une nouvelle licence.



Remarque
Veuillez noter que cette option n'est disponible que sous Windows 8.

Protection contre les logiciels espions et logiciels indésirables

Vous pouvez recevoir les remarques suivantes du Centre de maintenance Windows, concernant votre protection contre les logiciels espions et les logiciels indésirables :

- Avira Desktop indique qu'il est activé
- Windows Defender et Avira Desktop indiquent qu'ils sont tous deux désactivés
- Avira Desktop indique qu'il est périmé
- Windows Defender est périmé
- Windows Defender est désactivé

Avira Desktop indique qu'il est activé

Après l'installation de votre produit Avira et après une mise à jour effectuée ensuite, vous ne recevez tout d'abord aucun message du Centre de maintenance Windows. Cependant, sous **Centre de maintenance > Sécurité**, vous pouvez trouver les indications suivantes : *« Avira Desktop » indique qu'il est activé*. Cela signifie que votre produit Avira est à jour et que la protection temps réel est activée.



Windows Defender et Avira Desktop indiquent qu'ils sont tous deux désactivés

Vous recevez le message suivant si vous désactivez la protection temps réel Avira ou si vous arrêtez le service Protection temps réel.

Protection contre logiciels espions et programmes indésirables (important)
Windows Defender et Avira Desktop indiquent qu'ils sont tous deux désactivés.
Désactiver les messages concernant protection contre les logiciels espions
Afficher les programmes anti-e...

Remarque
Vous pouvez activer ou désactiver la **protection temps réel Avira** sous la rubrique **État** de l'**Avira Control Center**. Vous voyez en outre que la **protection temps réel Avira** est activée lorsque le parapluie rouge est ouvert dans votre barre des tâches. Il est également possible d'activer les différents composants Avira en cliquant sur *Activer maintenant* du Centre de maintenance. Si vous obtenez un message où vous devez donner votre accord pour lancer le programme Avira, cliquez sur *Autoriser*, et la protection temps réel est activée.

Avira Desktop indique qu'il est périmé

Si vous venez d'installer Avira, ou si pour une raison quelconque le fichier de définitions des virus, le moteur de recherche ou les fichiers de programme de votre produit Avira n'ont pas été mis à jour automatiquement (par ex. si vous mettez à jour votre système d'exploitation, sur lequel vous avez déjà installé votre produit Avira, pour passer d'une ancienne version de Windows à une nouvelle), le message suivant s'affiche :

Protection contre logiciels espions et programmes indésirables (important)
Avira Desktop indique qu'il est périmé.
Désactiver les messages concernant protection contre les logiciels espions
Mettre à jour
Télécharger un autre programme anti-espion

Remarque
Pour que le Centre de maintenance identifie votre produit Avira comme mis à jour, vous devez obligatoirement effectuer une mise à jour après l'installation. Vous actualisez votre système en exécutant une Mise à jour.



Windows Defender est périmé

Le message suivant peut apparaître lorsque Windows Defender est activé. Cela peut indiquer que votre produit Avira n'a pas été correctement installé. Veuillez vérifier l'installation.

Protection contre logiciels espions et programmes indésirables (important)
Windows Defender est périmé.
Mettre à jour
Désactiver les messages concernant protection contre les logiciels espions
Télécharger un autre programme anti-espion

> **Remarque**
> Windows Defender est la solution prédéfinie contre les logiciels espions et pour la protection antivirus de Windows.

Windows Defender est désactivé

Vous recevez le message du Centre de maintenance Windows *Windows Defender est désactivé* lorsqu'aucun logiciel de protection contre les logiciels espions n'a été trouvé sur votre ordinateur. Windows Defender est un logiciel intégré par défaut dans le système d'exploitation pour identifier les logiciels espions. Si vous avez installé un autre logiciel antivirus sur votre ordinateur, cette application est désactivée.
Si votre produit Avira a été correctement installé, vous ne recevez plus ce message, car le Centre de maintenance identifie automatiquement Avira. Vérifiez si Avira fonctionne correctement.

Protection contre logiciels espions et programmes indésirables (important)
Windows Defender est désactivé.
Activer maintenant
Désactiver les messages concernant protection contre les logiciels espions
Télécharger un autre programme anti-espion



15. Virus et autres

Avira Antivirus Suite identifie non seulement les virus et les logiciels malveillants, mais il peut également vous protéger contre d'autres dangers. Dans Ce chapitre, vous trouvez un aperçu des différents types de logiciels malveillants ainsi que des autres dangers encourus. Cette présentation décrit non seulement leur origine et leur comportement, mais également les mauvaises surprises qu'ils vous réservent.

Thèmes apparentés :

- Catégories de dangers
- Virus et autres logiciels malveillants

15.1 Catégories de dangers

Logiciels publicitaires

On appelle logiciel publicitaire un logiciel qui, en plus de sa fonctionnalité réelle, impose à l'utilisateur des bannières publicitaires ou fenêtres publicitaires intempestives. Ces affichages de publicités ne peuvent en général être désactivés et restent toujours visibles. Ici, les données de connexion permettent de tirer de nombreux renseignements sur le comportement d'utilisation et sont problématiques en matière de protection des données.

Votre produit Avira identifie les logiciels publicitaires. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels publicitaires** est activée, votre produit Avira vous avertit lorsqu'il détecte de tels logiciels.

Logiciels publicitaires/logiciels espions

Logiciel affichant de la publicité ou logiciel envoyant des informations personnelles de l'utilisateur à des tiers, le plus souvent sans son accord, ou à son issu, et qui est donc éventuellement indésirable.

Votre produit Avira identifie les logiciels publicitaires/espions. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels publicitaires/logiciels espions** est activée, votre produit Avira vous avertit lorsqu'il en détecte.

Application

L'appellation « Application » désigne une application dont l'utilisation peut être associée à un risque ou dont l'origine est douteuse.
Votre produit Avira détecte les applications (APPL). Si, dans la configuration, sous Catégories de dangers, l'option **Application** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de comportement.



Logiciels de commande Backdoor

Pour voler des données ou manipuler l'ordinateur, un programme de serveur backdoor passe par la « porte de derrière » sans que l'utilisateur ne le remarque. Via Internet ou le réseau, ce programme peut être commandé via un logiciel de commande backdoor (client) par des tiers.
Votre produit Avira détecte les logiciels de commande backdoor. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels de commande Backdoor** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de programme.

Fichiers à extensions déguisées

Fichiers exécutables qui déguisent leur extension de manière suspecte. Cette méthode de déguisement est souvent utilisée par les logiciels malveillants.
Votre produit Avira détecte les fichiers à extensions déguisées. Si, dans la configuration, sous Catégories de dangers, l'option **Fichiers à extensions déguisées** est activée, votre produit Avira vous avertit lorsqu'il en détecte.

Programme de numérotation payant

Certaines prestations de service sur Internet sont payantes. La facturation a lieu en Allemagne via les programmes de numérotation en 0190/0900 (en Autriche et en Suisse via des numéros en 09x0 ; en Allemagne le passage à des numéros en 09x0 aura lieu à moyen terme). Installés sur l'ordinateur, ces programmes, appelés dialers, assurent l'établissement de la connexion via un numéro surtaxé dont le prix peut être très variable.

La commercialisation de contenus en ligne via la facture téléphonique est légale et peut être avantageuse pour l'utilisateur. Les dialers sérieux affichent clairement leur utilisation consciente et réfléchie par le client. Ils ne s'installent sur l'ordinateur de l'utilisateur que si ce dernier a donné son accord, cet accord étant donné sur la base d'une présentation ou d'une incitation claires. L'établissement de la connexion via des programmes de numérotation sérieux s'affiche sans ambiguïté. En outre, les dialers sérieux indiquent clairement et avec précision les frais de connexion générés.

Malheureusement, il existe des dialers qui s'installent sur les ordinateurs de manière cachée et douteuse, voire à des fins frauduleuses. Ils remplacent par ex. la connexion de télétransmission standard de l'utilisateur Internet vers le FAI (fournisseur d'accès Internet) et appellent à chaque connexion un numéro en 0190/0900 surtaxé, parfois très cher. L'utilisateur ne remarque qu'après réception de la facture téléphonique suivante qu'un programme de numérotation indésirable en 0190/0900 a été utilisé sur son ordinateur à chaque connexion à Internet, avec pour conséquence des coûts très élevés.

Pour vous protéger des programmes de numérotation indésirables (dialers 0190/0900), nous vous conseillons de faire bloquer ce type de numéros directement auprès de votre opérateur téléphonique.

En général, votre produit Avira identifie les programmes de numérotation payants qu'il connaît.



Si, dans la configuration, sous Catégories de dangers, l'option **Programme de numérotation payant** est activée, votre produit Avira vous avertit lorsqu'il détecte un programme de ce type. Vous avez alors la possibilité de supprimer le programme de numérotation en 0190/0900. S'il s'agit d'un programme de numérotation souhaité, vous pouvez le déclarer comme fichier d'exclusion afin qu'il ne soit plus examiné à l'avenir.

Hameçonnage

L'hameçonnage, également connu sous le nom de « brand spoofing », est une forme raffinée de vol de données qui vise les clients ou clients potentiels des FAI, banques, services bancaires en lignes et autorités d'enregistrement.
Grâce à la transmission d'une adresse e-mail sur Internet, au remplissage de formulaires en ligne, à la participation à des groupes d'information ou par le biais de pages Web, il est possible que vos données soient volées par des « Internet crawling spiders » et utilisées sans votre accord pour une escroquerie ou d'autres forfaits.

Votre produit Avira détecte l'hameçonnage. Si, dans la configuration, sous Catégories de dangers, l'option **Hameçonnage** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de comportement.

Programmes portant atteinte à la vie privée

Logiciel qui compromet la sécurité de votre système, déclenche des activités de programmes non souhaitées, qui viole votre vie privée ou espionne votre comportement d'utilisateur et peut donc être indésirable.

Votre produit Avira détecte les logiciels de type « Security Privacy Risk ». Si, dans la configuration, sous Catégories de dangers, l'option **Programmes portant atteinte à la vie privée** est activée, votre programme Avira vous avertit lorsqu'il détecte des logiciels de ce type.

Programmes de blagues

Les programmes de blagues sont uniquement conçus pour effrayer ou pour amuser, sans être nuisibles ni se multiplier. Souvent, l'ordinateur joue une mélodie à l'ouverture du programme de blague ou affiche quelque chose d'inhabituel à l'écran. On peut citer à titre d'exemples la machine à laver dans le lecteur de disquettes (DRAIN.COM) et le mangeur d'écran (BUGSRES.COM).

Mais prudence ! Tous les signes des programmes de blagues peuvent aussi provenir d'un virus ou d'un cheval de Troie. Au mieux, vous en êtes quitte pour une belle frayeur, au pire la panique peut générer de véritables dégâts sur votre machine.

Votre produit Avira est capable de détecter les programmes de blagues grâce à l'élargissement de ses routines de recherche et d'identification, et le cas échéant, de les éliminer comme programmes indésirables. Si, dans la configuration, sous Catégories de dangers, l'option **Programmes de blagues** est activée, votre produit Avira vous avertit lorsqu'il détecte ce type de programmes.



Jeux

Les jeux sur ordinateur constituent une activité délassante, mais n'ont pas forcément leur place sur le lieu de travail (à part peut-être pour la pause déjeuner). Toutefois, dans les entreprises privées comme publiques, il n'est pas rare que les employés jouent. Internet permet de télécharger de nombreux jeux. Les jeux par e-mail aussi sont de plus en plus populaires : des simples échecs à la bataille navale, de nombreuses variantes circulent ; les jeux sont envoyés via les programmes de messagerie aux partenaires, qui répondent.

Des analyses ont montré que le temps de travail passé à jouer a atteint depuis longtemps des proportions économiques non négligeables. Il est d'autant plus compréhensible que de plus en plus d'entreprises décident de bannir les jeux des postes de travail.

Votre produit Avira identifie les jeux sur ordinateur. Si, dans la configuration, sous Catégories de dangers, l'option **Jeux** est activée, votre produit Avira vous avertit lorsqu'il détecte des jeux. Fin du jeu, au sens propre, car vous avez la possibilité de le supprimer.

Logiciels frauduleux

Également appelés « scareware » (logiciels destinés à effrayer) ou « rogueware » (logiciels fripouilles), il s'agit de logiciels frauduleux simulant des attaques virales et se proposant comme un logiciel antivirus professionnel. Le scareware est conçu pour inquiéter ou intimider l'utilisateur. Si la victime tombe dans le panneau et se pense menacée, elle se voit proposer contre paiement l'élimination du danger inexistant. Dans certains cas, la victime pensant être la cible d'une attaque est amenée à effectuer des manipulations qui elles, permettent alors une véritable attaque.

Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels frauduleux** est activée, votre produit Avira vous avertit lorsqu'il détecte un scareware.

Logiciels de compression inhabituels

Fichiers compressés avec un programme de compression inhabituel et qui peuvent donc être considérés comme suspects.

Votre produit Avira détecte les logiciels de compression inhabituels. Si, dans la configuration, sous Catégories de dangers, l'option **Logiciels de compression inhabituels** est activée, votre produit Avira vous avertit lorsqu'il détecte l'un de ces programmes.

15.2 Virus et autres logiciels malveillants

Logiciels publicitaires

On appelle logiciel publicitaire un logiciel qui, en plus de sa fonctionnalité réelle, impose à l'utilisateur des bannières publicitaires ou fenêtres publicitaires intempestives. Ces affichages de publicités ne peuvent en général être désactivés et restent toujours visibles.

Ici, les données de connexion permettent de tirer de nombreux renseignements sur le comportement d'utilisation et sont problématiques en matière de protection des données.

Backdoors

Un backdoor (porte de derrière en français) peut accéder à un ordinateur en contournant sa protection.

Un programme fonctionnant de manière cachée offre à un agresseur des droits quasi illimités. À l'aide du backdoor, il est possible d'espionner les données personnelles de l'utilisateur. Mais ils servent surtout à installer des virus ou vers sur le système concerné.

Virus d'amorçage

Le secteur d'amorçage ou le secteur d'amorçage maître des disques durs est infecté de préférence avec des virus d'amorçage. Ils écrasent des informations importantes pour le démarrage du système. L'une des conséquences désagréables est la suivante : le système d'exploitation ne peut plus être chargé...

Bot-Net

Un Bot-Net est un réseau commandable à distance (sur Internet) constitué de PC qui se composent de bots communiquant entre eux. Ce contrôle est obtenu par des virus ou chevaux de Troie qui contaminent l'ordinateur puis attendent des instructions sans faire de dégâts sur l'ordinateur infecté. Ces réseaux peuvent être utilisés pour répandre des spams, des attaques DDoS, etc., parfois sans que les utilisateurs des PC concernés ne le remarquent. Le principal potentiel des Bot-Nets est de pouvoir atteindre une taille de plusieurs milliers d'ordinateurs dont la somme des bandes passantes dépasse largement la plupart des accès à Internet traditionnels.

Exploit

Un exploit (lacune de sécurité) est un programme informatique ou script qui exploite les faiblesses spécifiques ou dysfonctionnements d'un système d'exploitation ou d'un programme. Comme exemple d'exploit, on peut citer les attaques en provenance d'Internet à l'aide de paquets de données manipulés qui exploitent les faiblesses dans le logiciel de réseau. Dans ce cas, des programmes peuvent être infiltrés, permettant d'obtenir un accès plus important.

Canulars (hoaxes en anglais)

Depuis quelques années, les utilisateurs d'Internet et d'autres réseaux reçoivent des alertes aux virus qui se répandent par e-mail. Ces avertissements sont transmis par e-mail avec la consigne de les transférer au plus grand nombre de collègues et d'utilisateurs possible pour les prévenir du danger.

Pot de miel

Un pot de miel (honeypot en anglais) est un service installé dans un réseau (programme ou serveur). Il a la tâche de surveiller un réseau et de consigner les attaques. Ce service est inconnu de l'utilisateur légitime et n'est donc jamais sollicité. Quand un agresseur recherche alors les points faibles d'un réseau et sollicite les services proposés par un pot de miel, il est enregistré et une alarme se déclenche.

Macrovirus

Les macrovirus sont des petits programmes écrits dans le macrolangage d'une application (par ex. WordBasic sous WinWord 6.0) et peuvent se répandre normalement dans les documents de cette application seulement. On les appelle donc également des virus documents. Pour être activés, ils nécessitent le démarrage de l'application correspondante et l'exécution de l'une des macros contaminées. Contrairement aux virus « normaux », les macrovirus n'infectent donc pas les fichiers exécutables mais les documents de l'application hôte.

Pharming

Le pharming est une manipulation du fichier hôte des navigateurs Web pour dévier les requêtes sur des sites Web falsifiés. Il s'agit d'une variante de l'hameçonnage. Les escrocs utilisant le pharming entretiennent leurs propres grandes fermes de serveurs sur lesquelles des sites Web falsifiés sont archivés. Le pharming s'est établi comme terme générique pour plusieurs types d'attaques DNS. En cas de manipulation du fichier hôte, une manipulation ciblée du système est entreprise, à l'aide d'un cheval de Troie ou d'un virus. Par conséquent, seuls les sites Web contrefaits sont encore accessibles par le système, même quand l'adresse Web a été correctement saisie.

Hameçonnage

L'hameçonnage est la « pêche » aux données personnelles de l'utilisateur d'Internet. L'hameçonneur envoie à sa victime des courriers d'apparence officielle, comme par exemple des e-mails l'incitant à communiquer sans méfiance des informations confidentielles, surtout des identifiants et mots de passe ou PIN et TAN pour les opérations bancaires en ligne. Avec les données d'accès volées, l'hameçonneur peut prendre l'identité de sa victime et agir en son nom. Une chose est certaine : les banques et assurances ne demandent jamais d'envoyer les numéros de cartes de crédit, PIN, TAN ou autres données d'accès par e-mail, SMS ou téléphone.

Virus polymorphes

Les virus polymorphes sont de véritables maîtres du camouflage et du déguisement. Ils modifient leurs propres codes de programmation et sont donc particulièrement difficiles à identifier.



Virus programmes

Un virus informatique est un programme capable de se lier à d'autres programmes et de les infecter, une fois qu'il a été ouvert. Les virus se multiplient donc seuls, contrairement aux bombes logiques et aux chevaux de Troie. Contrairement à un ver, le virus nécessite toujours un programme tiers comme hôte, dans lequel il dépose son code virulent. Toutefois, le déroulement même du programme de l'hôte n'est normalement pas modifié.

Rootkits

Un rootkit est un ensemble d'outils logiciels furtifs qui s'installent après avoir infiltré un système informatique, pour masquer la connexion de l'envahisseur, cacher des processus et récupérer des données - en résumé : pour se rendre invisible. Il essaie d'actualiser les programmes d'espionnage déjà installés et de réinstaller les logiciels espions supprimés.

Virus de script et vers

Ces virus sont extrêmement simples à programmer et se répandent - quand les conditions techniques sont réunies - par e-mail dans le monde entier en quelques heures.

Les virus et vers de script utilisent l'un des langages de script, par ex. Javascript, VBScript etc., pour s'insérer dans de nouveaux scripts ou se répandre par l'activation de fonctions du système d'exploitation. La contamination a souvent lieu par e-mail ou lors de l'échange de fichiers (documents).

On appelle ver un programme qui se multiplie sans contaminer d'hôte. Les vers ne peuvent donc pas devenir partie intégrante d'autres processus programmes. Les vers constituent souvent la seule possibilité d'infiltrer des programmes nuisibles sur les systèmes équipés de mesures de sécurité très strictes.

Logiciels espions

Les logiciels espions sont des programmes qui envoient les données personnelles de l'utilisateur à son insu et sans son accord au fabricant du logiciel ou à un tiers. La plupart du temps, les programmes espions servent à analyser le comportement de navigation de l'utilisateur sur Internet et à afficher des bannières ou fenêtres publicitaires intempestives ciblées.

Chevaux de Troie

Les chevaux de Troie sont devenus fréquents ces derniers temps. C'est ainsi que l'on appelle les programmes qui semblent avoir une fonction spéciale mais dévoilent leur véritable finalité après leur démarrage et exécutent une autre fonction souvent néfaste. Les chevaux de Troie ne peuvent pas se multiplier seuls, ce qui les différencie des virus et vers. La plupart portent un nom intéressant (SEX.EXE ou STARTME.EXE) pour inciter l'utilisateur à exécuter le cheval de Troie. Ils sont actifs dès l'exécution et formatent par

exemple le disque dur. Les droppers qui inoculent des virus dans un système informatique constituent un type particulier de cheval de Troie.

Logiciels frauduleux

Également appelés « scareware » (logiciels destinés à effrayer) ou « rogueware » (logiciels fripouilles), il s'agit de logiciels frauduleux simulant des attaques virales et se proposant comme un logiciel antivirus professionnel. Le scareware est conçu pour inquiéter ou intimider l'utilisateur. Si la victime tombe dans le panneau et se pense menacée, elle se voit proposer contre paiement l'élimination du danger inexistant. Dans certains cas, la victime pensant être la cible d'une attaque est amenée à effectuer des manipulations qui elles, permettent alors une véritable attaque.

Zombie

Un PC zombie est un ordinateur infecté par des programmes malveillants et qui permet aux pirates informatiques d'utiliser l'ordinateur à distance dans un but criminel. Le PC infecté lance sur demande, par exemple, des attaques de type Denial-of-Service (DoS) ou envoie des spams et des e-mails d'hameçonnage.

16. Info et service

16.1 Info et services

Ce chapitre vous informe sur l'info et les services proposés par Avira.

- Adresse de contact
- Support technique
- Fichier suspect
- Signaler une fausse alerte
- Vos réactions pour plus de sécurité

16.2 Adresse de contact

Nous serons heureux de vous aider en cas de questions et de suggestions concernant la gamme de produits Avira. Veuillez consulter le Control Center sous **Aide > À propos de Avira Antivirus Suite** pour obtenir nos adresses de contact.

16.3 Support technique

Avira est à vos côtés lorsqu'il s'agit de répondre à vos questions ou de résoudre un problème technique.

Vous trouverez toutes les informations nécessaires concernant notre service complet de support technique sur notre site Web :

http://www.avira.com/fr/support

Pour nous permettre de vous aider rapidement et de manière fiable, préparez les informations suivantes :

- **Données de licence**. Vous les trouverez dans l'interface du programme sous la rubrique **Aide > À propos de Avira Antivirus Suite > Informations de licence**. Voir Informations de licence.
- **Informations de version**. Vous trouverez ces informations sous la rubrique **Aide > À propos de Avira Antivirus Suite > Informations de version**. Voir Informations de version.
- **Version du système d'exploitation** et service packs éventuellement installés.
- **Packs logiciels installés**, par ex. logiciels antivirus d'autres fabricants.
- **Messages précis** du programme ou du fichier rapport.



16.4 Fichier suspect

Vous pouvez nous envoyer les fichiers suspects ou les virus qui ne peuvent pas encore être détectés ou supprimés par nos produits. Nous mettons plusieurs moyens à votre disposition.

- Identifiez le fichier dans le gestionnaire de quarantaine de Control Center de la console de sécurité du serveur Avira et sélectionnez l'élément **Envoyer fichier** via le menu contextuel ou le bouton correspondant.
- Envoyez le fichier requis compressé (WinZIP, PKZip, Arj, etc.) en pièce jointe à un e-mail à l'adresse suivante :
  virus@avira.com
  Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).
- Vous pouvez également nous envoyer le fichier suspect via notre site Web :
  http://www.avira.com/sample-upload

16.5 Signaler une fausse alerte

Si vous pensez que Avira Antivirus Suite signale une détection dans un fichier qui est probablement « propre », envoyez le fichier correspondant compressé (WinZIP, PKZip, Arj, etc.) en pièce jointe à un e-mail à l'adresse suivante :

virus@avira.com

Comme certaines passerelles de courrier électronique fonctionnent avec un logiciel antivirus, dotez le ou les fichier(s) d'un mot de passe (n'oubliez pas de nous communiquer ce mot de passe).

16.6 Vos réactions pour plus de sécurité

Chez Avira, la sécurité de nos clients est la première de nos préoccupations. Pour cette raison, nous ne nous appuyons pas seulement sur notre propre équipe interne d'experts qui fait subir à chaque solution Avira et à chaque mise à jour des tests de qualité et de sécurité poussés avant publication. Nous attachons également la plus grande importance à vos remarques sur d'éventuelles faiblesses de sécurité et nous les traitons ouvertement.

Si vous pensez avoir trouvé un point de vulnérabilité dans la sécurité de l'un de nos produits, merci d'envoyer un e-mail à l'adresse suivante :

vulnerabilities@avira.com